

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2022



KRAŠTO APSAUGOS
MINISTERIJA



NKC 
NACIONALINIS
KOORDINAVIMO CENTRAS
LIETUVA

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA 2022



KRAŠTO APSAUGOS
MINISTERIJA



NKC 
NACIONALINIS
KOORDINAVIMO CENTRAS
LIETUVA

Turinys



Dominančią temą galite pasiekti paspaudę ant jos pavadinimo



IŽANGA \04



SANTRAUKA \06



SVARBIAUSI 2022 M. ĮVYKIAI KIBERNETINIO SAUGUMO SRITYJE \16



PAGRINDINIAI ATASKAITOJE VARTOJAMI TERMINAI IR SĄVOKOS \18



KIBERNETINIO SAUGUMO APLINKOS STIPRINIMAS \22

ES gynybos iniciatyvų panaudojimas bendradarbiavimui \24

KAM veikla plėtojant bendradarbiavimą su strateginiais sąjungininkais ir partneriais Europoje \25

KAM veikla stiprinant Lietuvos pasirengimą reaguoti į įvairias grėsmes ir kibernetinės erdvės saugumą \27



LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA \30

Kibernetinių incidentų ir jų valdymo situacijos Lietuvoje apžvalga \31

Fiksuotų kibernetinių incidentų dinamika Lietuvoje \32

Karo Ukrainoje įtaka kibernetiniam saugumui \35

Kibernetinių incidentų prevencija ir kitos kibernetinį saugumą stiprinančios priemonės \37

Elektroninių ryšių tinklų vientisumo užtikrinimas ir draudžiamos viešai skleisti informacijos identifikavimas internete \40

RRT veikla, kuria prisidedama prie sklandaus interneto naudojimo \41

Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje \41

Interneto karštosios linijos „Švarus internetas“ veikla ir interneto svetainės www.esaugumas.lt administravimas \43

Viešųjų kompiuterių tinklų (internetu) prieigos vietose privalomų filtravimo priemonių naudojimo užtikrinimas \47

Karo Ukrainoje poveikis elektroninių ryšių tinklų saugumui \48

Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis \50

Nusikalstamų veikų kibernetinėje erdvėje mastas, poveikis ir tarptautinės tendencijos \51

Nusikaltimų kibernetinėje erdvėje Lietuvoje tendencijos \52

Kibernetiniai nusikaltimai plačiąja prasme \53

Kibernetiniai nusikaltimai siaurąja prasme \58

Kibernetinius nusikaltimus lėmusios aplinkybės ir kibernetinių nusikaltimų poveikio vertinimas \60

Naudojamos prevencinės priemonės \62

ADSP ir jų prevencijos priemonių apžvalga \64

Asmens duomenų apsaugos sąlygų lygis \65

ADSP Lietuvoje situacijos analizė \65

Tarptautinio bendradarbiavimo iniciatyvos ir mokymo bei švietimo veiklos \69

Priešiškos informacinės aplinkos apžvalga ir Lietuvos informacinės aplinkos saugumo vertinimas \70

Informacinės aplinkos grėsmių tendencijos \71

Prieš Lietuvos nacionalinius interesus vykdytos informacinės operacijos ir jų tendencijos \72

Informacinių incidentų skaičius pagal sritis \74

Informacinių incidentų naratyvai \76

Rezonansinės informacinės operacijos \77

01

Įžanga



Arvydas Anušauskas,
krašto apsaugos
ministras

2022-ieji pasižymėjo išskirtiniu įvykiu – karo sugrįžimu į Europos žemyną. 2022 m. vasario 24 d. Rusijos pradėta platus masto invazija į Ukrainą reikšmingai paveikė situaciją ne tik karo lauke, bet ir kibernetinėje erdvėje Ukrainoje ir už jos ribų. Karas Ukrainoje patvirtino, kad nebegalime kibernetinio saugumo laikyti atskira, izoliuota sritimi. Skaitmeninių technologijų amžiuje kibernetinis saugumas neatsiejamas nuo tradicinių saugumo pajėgumų, juos sustiprina arba, priešingai, susilpnina.

Kibernetinės atakos Rusijos kare prieš Ukrainą nuo pat jo pradžios užima svarbią vietą. Nors Rusija prieš Ukrainą kibernetines atakas vykdo jau nuo 2014 m., tačiau prieš pat 2022 m. vasario 24 d. invaziją šios atakos suintensyvėjo – sausio mėn. atakuotos Ukrainos vyriausybės institucijų svetainės ir jose paskleista paniką kelianti dezinformacija rusų, ukrainiečių ir lenkų kalbomis, o vasario mėn. paskirstytų paslaugų trikdymo atakomis ir pasitelkus duomenis naikinančią programinę įrangą atakuotos ne tik valstybinės informacinės sistemos, bet ir šalies energetikos, informacinių technologijų, žiniasklaidos ir finansų sektoriai. Šiomis atakomis buvo siekiama sustabdyti būtinųjų paslaugų teikimą gyventojams ir svarbiausia – pakirsti gyventojų pasitikėjimą Ukrainos valstybe, jos vadovybę ir silpninti valią priešintis. Per visą karo laikotarpį vykdyta kibernetinė puolamoji veikla apėmė bandymus sunaikinti ar įsiskverbti į Ukrainos valstybinių agentūrų tinklus ir daugybę ypatingos svarbos infrastruktūros objektų. Kai kuriais atvejais kibernetinės atakos prieš šiuos objektus buvo vykdomos kartu su Rusijos karinių pajėgų kinetinėmis atakomis.

Kare puolamieji kibernetiniai veiksmai neapsiribojo Ukrainos erdve. 2022 m. vasario 24 d. įvykdyta ataka prieš JAV palydovinio ryšio operatoriaus „Viasat“ valdomą palydovų tinklą KA-SAT sutrikdė interneto tiekimą ne tik Ukrainoje, bet ir Vokietijoje, Prancūzijoje, Vengrijoje, Graikijoje, Italijoje ir Lenkijoje. Už šios atakos įvykdymą ES pirmą kartą istorijoje viešai apkaltino Rusiją. Nors nuo karo pradžios Rusija pasitelkė didžiulius pajėgumus kibernetinei puolamajai veiklai, Ukraina sugebėjo atsilaikyti, o Vakarų partneriai susivienijo ir teikė jai visokeriopą pagalbą. Į Ukrainos gynybą stojo Ukrainos IT armija, sudaryta iš tarptautinių ir Ukrainos įsilaužėlių savanorių, bendradarbiaujančių su Ukrainos gynybos ministerijos pareigūnais ir vykdančių kibernetinius įsilaužimus į Rusijos infrastruktūros informacines valdymo sistemas bei Rusijos valstybės institucijų svetaines. Lietuva, Nyderlandai, Lenkija, Estija, Rumunija ir Kroatija 2022 m. vasario 22 d. aktyvavo ES Kibernetinės greitojo reagavimo pajėgas, reaguodamos į Ukrainos užsienio reikalų ministro Dmytro Kulebos 2022 m. vasario 18 d. kreipimąsi į ES institucijų ir valstybių narių atstovus su kibernetinės paramos prašymu. 2022 m. liepos 19 d. Lietuvos iniciatyva paskelbta bendra ES deklaracija dėl prieš Lietuvą ir kitas Europos šalis nukreiptų prorusiškų kibernetinių programinių atakų Rusijos karo Ukrainoje kontekste.

2022 m. prasidėjęs karas Ukrainoje parodė, kad tarptautinė sistema tampa vis sunkiau prognozuojama. Lietuva ir kitos regiono šalys privalo neprarasti budrumo ir prisitaikyti prie pokyčių pasaulyje ir regione. Tai reiškia, kad Lietuva turi ne tik toliau vystyti savo gynybos pajėgumus, bet ir dar aktyviau bendradarbiauti su strateginiais partneriais bei didinti valstybės ir visuomenės atsparumą kylančioms grėsmėms.

Nacionalinio kibernetinio saugumo centro duomenimis, kaimynystėje vykstantis karas palietė ir Lietuvos kibernetinę erdvę. Nors 2022 m. Nacionalinio kibernetinio saugumo centro registruotų kibernetinių incidentų skaičius išliko panašus kaip ir 2021 m., tačiau paskirstytų paslaugų trikdymo atakų skaičius išaugo. 2022 m. birželio mėn. paskirstytų paslaugų trikdymo atakomis taikytasi į Lietuvos viešojo ir privataus sektoriaus svetaines. Per atakas, už kurias atsakomybę prisiėmė Rusijos Federacijos politiką palaikanti įsilaužėlių grupuotė, bandyta paveikti daugiau nei 130 viešai pasiekiamų interneto svetainių. Svarbu pažymėti, kad Lietuva šį kibernetinį išpuolį ne tik atlaikė (žalos svetainėms nebuvo padaryta), bet ir tapo stipresnė, skiria dar daugiau dėmesio savo kibernetinės erdvės apsaugai.

Kibernetinio saugumo būklė susijusi ir su kibernetinių nusikaltimų skaičiumi: 2022 m. nusikalstamumas kibernetinėje erdvėje, palyginti su 2021 m., išaugo net 52 proc., o pagrindinis motyvas liko nusikalstamas pelnymas. 2022 m. finansiniams sukčiams iš Lietuvos gyventojų ir įmonių pavyko išvilioti beveik 12 mln. eurų.

2022-ieji ir Lietuvos informacinėje erdvėje buvo išskirtiniai metai – Lietuvos gynybos ir užsienio politikos temos buvo išnaudojamos Kremliaus ir Baltarusijos režimų propagandos tikslais. Tai sutapo su reikšmingais užsienio ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti neigiamam šalies įvaizdžiui Vakaruose kurti ir Lietuvos visuomenės auditorijų tarpusavio susipriešinimui skatinti. Svarbu pabrėžti, kad Lietuvos visuomenė ir informacinė erdvė išlieka atspari Rusijos transliuojamiems naratyvams, o viešųjų ryšių tinklų pajėgumai, kurie būtini darniam valstybės funkcionavimui ir kibernetinės erdvės saugumui užtikrinti, Lietuvoje taip pat yra pakankami, nuolatos stebimi bei atsakingai vertinami. Artėjant Bendrojo duomenų apsaugos reglamento 5-osioms metinėms, verta pažymėti, kad žmonės, netinkamai tvarkančios asmens duomenis, yra išaiškinamos ir nubaudžiamos, o duomenų valdytojai įgyja vis daugiau žinių, didėja jų sąmoningumas asmens duomenų apsaugos srityje.

Didėjantis kibernetinio saugumo poreikis sudarė pagrindą ES kurti teisinę bazę savo piliečių ir įmonių kibernetiniam saugumui užtikrinti. Nuo 2013 m., kai buvo priimta pirmoji, o 2020 m. ir antroji ES kibernetinio saugumo strategija, ES pateikė ne vieną naują siūlymą, kaip dar labiau padidinti kibernetinės erdvės saugumą. Antroji Tinklų ir informacinių sistemų direktyva, naujausias Europos Komisijos pasiūlymas dėl Kibernetinio atsparumo akto ir kitos tiekimo grandinės saugumo užtikrinimui reikalingos iniciatyvos įrodo, kad kibernetinis saugumas yra vienas iš ES politikos formuotojų prioritetų. Pamatinių Lietuvos valstybės ir visuomenės teisių ir laisvių užtikrinimas kibernetinėje erdvėje yra ir Krašto apsaugos ministerijos prioritetas. Siekiant užtikrinti tiekimo grandinių saugumą, Krašto apsaugos ministerijos iniciatyva pateikti ir 2022 m. kovo mėn. priimti teisės aktai, užtikrinantys, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga. Be to, šiuo metu rengiama ir aiškius kibernetinio saugumo tikslus iki 2030 m. įtvirtinsianti Nacionalinė kibernetinio saugumo plėtros programa, pagal kurią kibernetinio saugumo priemonės skiriami finansai leis dar efektyviau įgyvendinti numatytas priemones.

Noriu padėkoti visoms institucijoms, kurios jau trečius metus iš eilės prisideda rengiant šią Nacionalinę kibernetinio saugumo būklės ataskaitą, – Nacionaliniam kibernetinio saugumo centrui, Valstybinei duomenų apsaugos inspekcijai, Lietuvos policijai, Ryšių reguliavimo tarnybai, Lietuvos kariuomenės Strateginės komunikacijos departamentui. Šis bendradarbiavimas ir dalijimasis žvalgomis leidžia pristatyti išsamesnį kibernetinio saugumo grėsmių žemėlapią bei bendromis jėgomis kurti saugesnę kibernetinio saugumo aplinką Lietuvoje.

02

Santrauka



1 Kibernetinio saugumo grėsmės, priešišų valstybių interesai bei visuomenės atsparumo įtaka Lietuvos kibernetinio saugumo būklei

1. 2022 m. Lietuvoje buvo toliau stiprinamas perkančiųjų organizacijų tiekimo grandinės saugumas, tęstas Nacionalinės kibernetinio saugumo plėtros programos (toliau – Programa) rengimas, patvirtintas informacinių išteklių prieinamumą ir atkūrimą reglamentuojantis tvarkos aprašas.

2022 m. įsigaliojo teisės aktai, užtikrinantys, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga. Priimti Lietuvos Respublikos viešųjų pirkimų įstatymo⁰¹, Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo⁰², Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymo⁰³ pakeitimai, kuriais siekiama valdyti rizikas, kylančias nacionaliniam saugumui dėl nesaugių (nepatikimų) informacinių technologijų naudojimo kritinėje valstybės infrastruktūroje.

2022 m. tęstas 2021 m. pradėtos Programos rengimas, į jos įgyvendinimą įtraukiamos įvairios valstybės institucijos. Planuojama dalį Programos veiklų finansuoti Ekonomikos gaivinimo ir atsparumo didinimo plano „Naujos kartos Lietuva“ lėšomis ir skirti 40,15 mln. eurų.

Krašto apsaugos ministerija (toliau – KAM) dalyvavo rengiant Valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašą, jį patvirtino Vyriausybė 2022 m. liepos 11 d. nutarimu Nr. 739⁰⁴. Šis tvarkos aprašas nustato Lietuvos Respublikos Vyriausybės įgaliotos institucijos ir į Vyriausybės nutarimu patvirtintą sąrašą įtrauktų registrų ir valstybės informacinių sistemų valdytojų ir šių sistemų tvarkytojų veiksmus, siekiant užtikrinti, kad valstybės informaciniai ištekliai būtų prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, ir taip garantuoti jų apsaugą.

2. Tarptautinis bendradarbiavimas kibernetinio saugumo gynybos srityje ir toliau lieka vienas iš Lietuvos prioritetų siekiant stiprinti nacionalinius ir regioninius pajėgumus.

KAM 2022 m. lapkričio 7 d. Lietuvoje kartu su Europos Sąjungos (toliau – ES) Tarybai pirminin-kaujančios Čekijos ir ES kibernetinio saugumo agentūros (angl. *European Union Agency for Cybersecurity*, ENISA) (toliau – ENISA) atstovais surengė kasmetines krizių valdymo pratybas „BlueOLEX 2022“, skirtas Europos ryšių palaikymo Kibernetinių krizių organizacinio tinklo (angl. *Cyber Crisis Liaison Organisation Network* (CyCLONE)) operacinių veikimo procedūroms testuoti ir tobulinti. 2022 m. Vilniuje vykusiose pratybose dalyvavo atstovai iš 22 ES valstybių narių, taip pat iš Europos Komisijos ir ENISA.



01

Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 25, 27, 35, 37, 39, 45, 47, 51, 90 ir 92 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/0ed02bd3a5ff11ecaf79c2120caf5094?positionInSearchResults=1&searchModelUUID=90d1a3c6-7c67-4c0e-8293-f08f9cb05fd0>.

02

Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo Nr. XIII-328 2, 29, 37, 39, 48, 50, 52, 58, 98 ir 100 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/409b3602a5ff11ecaf79c2120caf5094?positionInSearchResults=0&searchModelUUID=c763dc84-b132-4afa-ac32-baad3018a0f2>.

03

Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo Nr. XIII-328 2, 29, 37, 39, 48, 50, 52, 58, 98 ir 100 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/409b3602a5ff11ecaf79c2120caf5094?positionInSearchResults=0&searchModelUUID=c763dc84-b132-4afa-ac32-baad3018a0f2>.

04

Valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/779cbbc401a711edbf9c72e552dd5bd?positionInSearchResults=6&searchModelUUID=0a605674-93d7-4635-acf9-7c35ea7543a7>.

2022 m. veiklą pradėjo Nacionalinis koordinavimo centras (toliau – NKC), kurio užduotis nuo 2022 m. pradžios pradėjo vykdyti KAM pagal 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentą (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas⁰⁵. Šio tinklo sudedamąja dalimi tampa Lietuvos NKC, o jam talkina partneriai: Nacionalinis kibernetinio saugumo centras prie KAM (toliau – NKSC), VŠĮ Inovacijų agentūra bei VŠĮ Centrinė projektų valdymo agentūra. Naudodamas „Skaitmeninės Europos“ programos bei Lietuvos Respublikos valstybės biudžeto lėšas, 2023 m. pab. Lietuvos NKC skelbs kvietimus mažų ir vidutinių įmonių (toliau – MVĮ) projektų kibernetinio saugumo inovacijų srityse finansavimui iki 60 tūkst. eurų gauti (pavyzdžiui, kibernetinio saugumo sprendimams „EdTech“ srityje ir kibernetinio saugumo sprendimams MVĮ atsparumui didinti). Lietuvos NKC taip pat vykdys kitas visiems ES šalyse veikiantiems NKC būdingas veiklas, tokias kaip kibernetinio saugumo kultūros skatinimas, Lietuvos kibernetinio saugumo bendruomenės formavimas ir informavimas, kibernetinio saugumo švietimo programų propagavimas ir sklaida, dalijimasis ekspertinėmis kibernetinio saugumo žiniomis.

2022 m. toliau buvo vykdoma Regioninio kibernetinės gynybos centro (toliau – RKGK), kuris veikia kaip NKSC filialas, plėtra. RKGK parengė ir su partneriais pasidalino daugiau kaip 40 kibernetinių grėsmių žvalgybos ataskaitų bei kibernetinių įvykių analizių. Iš parengtų dokumentų buvo galima aiškiau suprasti aktualiausius regiono kibernetinius incidentus.

Taip pat buvo parengta Ukrainos kariuomenės kadetų praktikos mokymo programa ir baigtas bandomasis kursas. 2023 m. pradėta vykdyti Ukrainos kadetų praktikos programa RKGK leis jiems įgyti vertingų praktinių žinių bei jas panaudoti tarnyboje, taip pat tai vienas iš Lietuvos paramos būdų kovojančiai Ukrainai.

Stiprindami regioninį bendradarbiavimą, 2022 m. gegužės mėn. NKSC pasirašė dvišalio bendradarbiavimo susitarimą (angl. *Memorandum Of Understanding*) su Lenkijos Nacionalinio kibernetinio saugumo centru – kibernetine vadaviete, o Lietuvos ir Lenkijos komanda užėmė antrąją vietą (iš 24) didžiausiose pasaulyje kibernetinės gynybos pratybose „Locked Shields 2022“. 2022 m. rudenį buvo priimtas sprendimas dėl Lenkijos prisijungimo prie RKGK, o 2023 m. sausio mėn., pasirašius reikiamus susitarimus, Lenkija tapo RKGK nare.

2022 m. pavasarį NKSC specialistai kartu su JAV kariuomenės kibernetinės vadavietės atstovais sėkmingai įvykdė kibernetinės gynybos operaciją „Hunt Forward“, kurios pagrindinis tikslas buvo stiprinti praktinį sąveikumą ir didinti svarbiausių tinklų atsparumą kibernetinėms grėsmėms. 2021–2022 m. Lietuva taip pat dalyvavo JAV kuruojamoje tarptautinėje iniciatyvoje prieš išpirkos reikalaujančias atakas (angl. *Counter Ransomware Initiative*), kurios tikslas – suvienyti 36 šalių pastangas kovojant prieš Rusijos ir kitų šalių organizuojamas išpirkos reikalaujančias atakas, stiprinti tinklų atsparumą ir griauti nusikalstamų grupuočių infrastruktūrą.

3. Rusijos invazijos į Ukrainą fone ES dėl išaugusių kibernetinio saugumo grėsmių ėmėsi veiksmų, siekdama suteikti pagalbą Ukrainai bei užsitikrinti savo kibernetinės erdvės saugumą.

Nuo pat 2022 m. pradžios kibernetinės atakos buvo neatsiejama Rusijos karinės agresijos prieš Ukrainą dalis. Atakos turėjo poveikį ne tik Ukrainai, bet ir kitoms ES ir NATO valstybėms. ES kibernetinė darbotvarkė 2022 m. koncentruota į ES ir ES valstybių narių visapusiškos paramos Ukrainai teikimą ir ES teisėkūros pasiūlymų kibernetinio saugumo srityje derinimą. 2022 m. Lietuva kartu su kitomis ES valstybėmis narėmis aktyviai teikė Ukrainai kibernetinio saugumo paramą, įskaitant įrangos ir programinės įrangos (PI) teikimą.



05

2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32021R0887&from=EN>.

Lietuva, Nyderlandai, Lenkija, Estija, Rumunija ir Kroatija 2022 m. vasario 22 d. aktyvavo ES Kibernetinės greitojo reagavimo pajėgas (angl. *Cyber Rapid Response Teams* (CRRT))⁰⁶, reaguodamos į Ukrainos užsienio reikalų ministro Dmytro Kulebos 2022 m. vasario 18 d. kreipimąsi į ES institucijų ir valstybių narių atstovus su kibernetinės paramos prašymu. ES Kibernetinės greitojo reagavimo pajėgos 2022 m. lapkričio mėn. teikė paramą Moldovoje ir atliko pažeidžiamumų vertinimą⁰⁷.

2022 m. gegužės 10 d. ES pirmą kartą istorijoje oficialiai priskyrė kibernetinę ataką Rusijai, nes ši, likus kelioms valandoms iki masinio įsiveržimo į Ukrainą, įvykdė kibernetinę ataką prieš JAV palydovinio ryšio operatoriaus „Viasat“ valdomą palydovų tinklą KA-SAT. Dėl šios atakos sutriko interneto tiekimas ne tik Ukrainoje, bet ir Vokietijoje, Prancūzijoje, Vengrijoje, Graikijoje, Italijoje ir Lenkijoje. Lietuvos iniciatyva 2022 m. liepos 19 d. taip pat paskelbta bendra ES deklaracija dėl prieš Lietuvą ir kitas Europos šalis nukreiptų prorusiškų kibernetinių programišių atakų Rusijos karo Ukrainoje kontekste.

Siekdamos atgrasyti iš trečiųjų šalių ar nusikalstamų veikėjų kylančias kibernetines grėsmes ir atakas ES ir ES valstybėms narėms, ES Taryba 2022 m. gegužę iki 2025 m. pratęsė ir nustatė ilgesnį, trejų metų trukmės, kibernetinių ribojamųjų priemonių sistemos galiojimą. Pagal šią sistemą ES gali taikyti tikslines ribojamąsias priemones su kibernetiniais išpuoliais susijusiems asmenims ar subjektams, kurie daro didelį poveikį ir kelia išorės grėsmę ES ar jos valstybėms narėms. Šiuo metu kibernetinių sankcijų sąrašė yra aštuoni asmenys ir keturi subjektai iš Rusijos, Kinijos ir Šiaurės Korėjos.

4. 2022 m. ES teisėkūros iniciatyvos kibernetinio saugumo srityje buvo daugiausia orientuotos į aukšto bendro kibernetinio saugumo lygio didinimą, aparatinės ir programinės įrangos produktų saugumą.

Po dvejus metus trukusių derybų 2022 m. gruodžio 27 d. oficialiajame ES leidinyje paskelbta Direktyva dėl priemonių, skirtų aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje (angl. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, (NIS2)*) (toliau – NIS2 direktyva)⁰⁸, kuri sustiprins viešojo ir privataus sektoriaus bei visos ES kibernetinį atsparumą ir reagavimo į incidentus pajėgumus. NIS2 direktyva įsigaliojo 2023 m. sausio 16 d., šio ES teisės akto nuostatomis perkelti valstybėms narėms skirtas 21 mėnuo.

2022 m. rugsėjo 15 d. Europos Komisija taip pat pateikė naują ES reglamento pasiūlymą dėl Kibernetinio atsparumo akto (angl. *Cyber Resilience Act*, CRA). Teisės aktu siekiama nustatyti horizontaliuosius privalomus kibernetinio saugumo reikalavimus techninės ir programinės įrangos produktams visam jų gyvavimo ciklui. Lietuva, kaip ir kitos ES valstybės, sutinka, kad į ES rinką patektų tik aukščiausius atsparumo, apsaugos ir saugumo standartus atitinkančios technologijos, o prasidėjusiose ES Tarybos derybose tikslinamos teisės akto pasiūlymo nuostatos.



06

Kibernetinės greitojo reagavimo pajėgos veikia pagal Lietuvos vadovaujamą ES nuolatinio struktūrizuoto bendradarbiavimo (angl. *Permanent Structured Cooperation*, PESCO) projektą.

07

2023 m. kovo mėn. ES Kibernetinės greitojo reagavimo pajėgos teikė paramą ES karinėje misijoje Mozambike ir atliko pažeidžiamumų vertinimą.

08

NIS2 direktyva, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=lt>.



5. 2022 m. NKSC incidentų valdymo skyrius (toliau – CERT-LT) iš viso užregistravo 4 080 kibernetinių incidentų, jų skaičius išliko panašus, kaip ir 2021 m. Priešingai nei ankstesniais metais, išaugo paskirstytų paslaugų trikdymo (angl. *Distributed Denial of Services*, DDoS) (toliau – DDoS) atakų skaičius.

CERT-LT 2022 m. iš viso užregistravo 4 080 kibernetinių incidentų, t. y. 8 incidentais mažiau nei 2021 m. Iš visų 2022 m. fiksuotų incidentų 33 priklauso vidutinei kategorijai ir yra susiję su DDoS atakomis ir kenksmingo programinio kodo, skirto prieigai prie ryšių informacinių sistemų gauti ir kenkimo veiklai (pavyzdžiui, šnipinėjimą ir kitus destruktivius veiksmus) vykdyti, platinimu. Palyginti su 2021 m., 2022 m. vidutinės kategorijos incidentų skaičius sumažėjo 35 proc. (2021 m. – 93 atvejai).

Apžvelgiant visus 2022 m. NKSC fiksuotus kibernetinius incidentus, kaip ir prieš metus, daugiausia incidentų buvo susiję su kenkimo programinės įrangos platinimu, socialinės inžinerijos atakomis, kuriomis siekta išvilioti įvairius jautrius duomenis (angl. *phishing*), nepageidaujamos informacijos platinimu, mėginimais įsilaužti. Tačiau, priešingai nei ankstesniais metais, išaugo DDoS atakų skaičius.

2022 m. birželio pab. NKSC fiksavo didžiulę DDoS atakų prieš viešąjį ir privatų sektorius bangą. Iš viešųjų šaltinių buvo surinkta informacija apie bandymus paveikti daugiau kaip 130 viešai pasiekiamų interneto svetainių. Atsakomybę už vykdytas atakas prisiėmė Rusijos Federacijos politiką palaikanti įsilaužėlių grupuotė. Atakos bendrovių informacinėms sistemoms žalos nepadarė, pastebėtas net teigiamas poveikis – informacinių sistemų tvarkytojai ir valdytojai pradėjo skirti daugiau dėmesio ir finansų savo kibernetinio saugumo stiprinimui.

Panašios kibernetinių incidentų tendencijos fiksuojamos ir Europoje. Remiantis ENISA metine grėsmių apžvalga⁰⁹, pagal dažnumą antroje vietoje yra kenkimo PJ, o trečiojoje vietoje – informacijos rinkimas naudojant socialinės inžinerijos įrankius. Pasak ENISA, Europoje duomenis šifruojančio kenksmingo programinio kodo (angl. *ransomware*) atakos yra vienas iš dažniausiai Europoje pasitaikančių kibernetinių incidentų tipų.

Lietuvoje daugiausia kibernetinių incidentų 2022 m., kaip ir ankstesniais metais, fiksuota prieglobos paslaugų teikėjų infrastruktūrose, kurias galima naudoti interneto svetainėms, virtualioms darbo vietoms, el. pašto paslaugoms kurti ir pan. Tokį didelį incidentų skaičių nulėmė dvi priežastys: pažeidžiamos interneto svetainės ir galimybė Lietuvoje anonimiškai įsigyti prieglobos paslaugas. Be to, dažnai prieglobos teikėjai sudaro galimybę už paslaugas atsiskaityti kriptovaliuta, o tai pirkėjams sukuria anonimiškumą ir apsunkina jų atsekamumą arba padaro jį iš viso neįmanomą.

6. Karo poveikis Ukrainos kibernetinio saugumo aplinkai.

Nuo 2014 m. Rusijos prieš Ukrainą vykdytos kibernetinės atakos prieš karą suintensyvėjo. 2022 m. sausio 13–14 d. atakuota daugiau kaip 70 Ukrainos vyriausybinių institucijų svetainių ir jose paskleista dezinformacija rusų, ukrainiečių ir lenkų kalbomis. Išpuoliai tęsėsi ir vasario mėn., o likus kelioms dienoms iki karinės invazijos pradžios surengtos dvi masinės kibernetinės atakos. 2023 m. vasario 16 d. prieš šimtus Ukrainos interneto svetainių surengta DDoS ataka, o vėliau įvykdyta ataka duomenis naikinančia PJ (angl. *wiper malware*) prieš šimtus Ukrainos valstybinių informacinių sistemų, taip pat šalies energetikos, informacinių technologijų, žiniasklaidos ir finansų sektorius. Pagrindinis šių atakų tikslas buvo pakirsti gyventojų pasitikėjimą Ukrainos valstybe ir vadovais bei silpninti gyventojų valią priešintis.



Ukrainos kibernetinių incidentų valdymo komandos CERT-UA duomenimis, nuo masinės invazijos į Ukrainą pradžios 2022 m. vasario 24 d. iki 2023 m. vasario 1 d. iš viso užregistruoti 2 245 incidentai: kenkimo PJ panaudojimo atvejų (568), informacijos rinkimo (angl. *phishing*) (552) ir sėkmingų įsilaužimų (394). Daugiausia kibernetinių incidentų užregistruota valstybės ir savivaldybių srityje veikiančių organizacijų infrastruktūroje (564), saugumo ir gynybos srityje (312) bei verslo srityje (159).

Karas taip pat turėjo įtakos kibernetinių aktyvistų (angl. *hacktivists*) grupuočių, kurios stojo į priešingą kariaujančių šalių puses ir aktyviai ėmė jas remti, veiklai. Ukrainą remiančios kibernetinių aktyvistų grupuotės, tokios kaip Ukrainos IT armija, skelbėsi įsilaužusios į svarbiausias Rusijos valdžios institucijas ir gavusios prieigą prie didžiulės apimties svarbios informacijos, sutrikdžiusios pagrindinių žiniasklaidos priemonių veiklą ir įvykdžiusios kitus žalingus veiksmus. Tuo metu prorusiška aktyvistų grupuotė daugiausia skelbė apie didesnes ar mažesnes DDoS atakas tiek Europoje, tiek JAV.

Kibernetiniai išpuoliai prieš kritinę Ukrainos infrastruktūrą buvo vykdomi visus 2022 m. Karo pradžioje kibernetinės atakos buvo sudėtingesnės, joms rengtasi iš anksto, kartais net iki 6 mėn. Vėlesnių išpuolių atakos buvo paprastesnės, pavyzdžiui, DDoS atakos, socialinės inžinerijos principais paremti bandymai išvilioti jautrius duomenis, dezinformacijos platinimas ir pan.

7. Reaguodamas į įvykius Ukrainoje ir pasikeitusią kibernetinio saugumo aplinką, NKSC aktyviai teikė rekomendacijas ir nurodymus kritinės infrastruktūros valdytojams dėl prevencinių kibernetinio saugumo priemonių taikymo, ypač daug dėmesio skyrė veiklos tęstinumo planams ir mokymams.

2022 m. balandžio mėn. buvo surengtos pratybos, išbandytas Saugusis valstybinis duomenų perdavimo tinklas ir įvertinti institucijų gebėjimai juo naudotis nutrūkus tarptautiniam interneto ryšiui¹⁰. Siekiant užtikrinti operatyvų informacijos apsikeitimą ir reagavimą į galimas grėsmes tarp kibernetinio saugumo subjektų ir NKSC, Kibernetinio saugumo informaciniame tinkle (toliau – KSIT) buvo sukurta uždara pokalbių platforma ir duomenų apsikeitimo modulis.

Valstybės ir ypatingos svarbos informacinės infrastruktūros darbuotojai taip pat buvo skatinami atsakingai įvertinti padidėjusias kibernetinio saugumo rizikas. Tam NKSC skyrė ypač daug dėmesio – daugiau nei 1 200 valstybės ir savivaldybių darbuotojų baigė kompleksinius trijų dienų kibernetinio saugumo mokymus, o 2 400 valstybės tarnautojų išklause NKSC trumpesnius mokymus įvairiomis bazinių kibernetinio saugumo žinių temomis. Specialus kursas organizuotas ir paramą Ukrainai renkančioms Lietuvos organizacijoms.

NKSC, bendradarbiaudamas su Kauno technologijų universitetu (toliau – KTU), surengė iki šiol didžiausias pagal dalyvių skaičių nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2022“, jose dalyvavo 116 organizacijų, iš jų 107 – valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai. Naudojantis NKSC įdiegtu socialinės inžinerijos įrankiu „GoPhish“ išsiųsti kibernetinių sukčių žinutes imituojantys el. laiškai, jų neatpažino ir žalingus veiksmus atliko beveik 13 proc. darbuotojų. Tai rodo būtinybę vykdyti nuolatinį darbuotojų švietimą.



Iš viso per metus poligono galimybėmis pasinaudojo ir savo profesines žinias sustiprino 163 Lietuvos ir 58 užsienio partnerių darbuotojai iš 47 organizacijų. Kibernetinio saugumo treniruoklis buvo panaudotas ir nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas 2022“. Šia galimybe pasinaudojo 92 dalyviai iš 25 organizacijų.

2022 m. NKSC koordinavo Lietuvos kibernetinio saugumo subjektų dalyvavimą didžiausiose ES kibernetinio saugumo pratybose „CyberEurope 2022“. Jose dalyvavo 8 didžiausios šalies asmens sveikatos priežiūros įstaigos, taip pat NKSC, Sveikatos apsaugos ministerija ir Registrų centras. Kovai su žaibiškėmis kibernetinėmis sukčiavimo atakomis NKSC kartu su KTU Interneto paslaugų centru DOMREG sukūrė ir 2022 m. rudenį pristatė naują nemokamą įrankį gyventojams ir organizacijoms – DNS užkardą. Iki metų pabaigos ją savanoriškai įsidiegė ne tik gyventojai ir verslo organizacijos, bet ir dalis ypatingos svarbos informacinės infrastruktūros valdytojų.



8. NKSC vykdė ypatingos svarbos informacinių išteklių tikrinimus bei kibernetinių grėsmių paiešką kibernetinio saugumo subjektų tinkluose.

NKSC 2022 m. pradėjo vykdyti kibernetinių grėsmių paiešką kibernetinio saugumo subjektų tinkluose. Per pirmuosius šios veiklos metus nustatytos 184 potencialios grėsmės ir apie jas kibernetinio saugumo subjektai informuoti tiesiogiai arba per interneto paslaugų teikėjus.

Buvo toliau nuosekliai vykdoma atsakingo atskleidimo koordinavimo veikla, o per 2022 m. NKSC sulaukė 51 pranešimo iš kibernetinio saugumo specialistų apie galimas spragas valstybinių institucijų interneto svetainėse. Buvo gauta vertingos informacijos apie svarbių sistemų saugumo spragas, tarp kurių viešajame sektoriuje populiarų dokumentų valdymo sistema „Avily“ bei viešojo sektoriaus valdomos informacinės sistemos. 2021 m., laikydamasis atsakingo atskleidimo principų, NKSC gavo 81 pranešimą apie įvairias kibernetinio saugumo spragas.

NKSC vykdė ypatingos svarbos informacinių išteklių patikrinimus, siekdamas nustatyti, kaip ypatingos svarbos informacinių išteklių valdytojai laikosi organizacinių ir techninių kibernetinio saugumo reikalavimų (toliau – OTR). Per metus atlikti 6 patikrinimai (1 iš jų pakartotinis) energetikos, susisiekimo, civilinės saugos ir vandens tiekimo sektoriuose (2021 m. atlikti 5 patikrinimai).

Per metus NKSC įvertino 279 valstybės informacinių išteklių saugos dokumentų, iš kurių 199 buvo patvirtinti, dėl kitų pateiktos pastabos. Siekiant patikrinti, kaip valstybės informacinių išteklių valdytojas laikosi saugos dokumentų reikalavimų, 2022 m. buvo atliktas vienas bandomasis valstybės informacinių išteklių valdytojo patikrinimas. Siekiama, kad NKSC būtų suteiktos teisės nuolatos atlikti valstybės informacinių išteklių patikrinimus.



9. Ryšių reguliavimo tarnybos (toliau – RRT) teigimu, viešųjų ryšių tinklų pajėgumai buvo ir yra pakankami, tinklai ir toliau atsakingai planuojami, stebimi bei vertinami.

2022 m. RRT iš trijų teikėjų gavo 7 pranešimus (2021 m. – 8 pranešimus) apie viešųjų ryšių tinklų vientisumo pažeidimus. Nepaisant vieno didesnio masto viešųjų ryšių tinklų vientisumo pažeidimo, viešųjų ryšių tinklų pajėgumai buvo ir yra pakankami, taip pat tinklai planuojami ir stebimi bei vertinami atsakingai. Tokia išvada daroma iš teikėjų RRT pateiktų pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus, kas 3 mėnesius gaunamos papildomos informacijos ir papildomai įvertinus RRT atliekamų viešųjų elektroninių ryšių paslaugų kokybės matavimo rodiklius nuolatinės stebėsenos metu.

Viešojo mobiliojo ir viešojo fiksuotojo ryšio tinkluose 2022 m. nebuvo fiksuojama daugiau gedimų nei ankstesniais metais, fiksuoti gedimai pašalinti operatyviai, o viešųjų ryšių tinklų vientisumo pažeidimų mastas nesukėlė ekstremalių įvykių, dėl kurių būtų reikėję imtis papildomų veiksmų ir (ar) informuoti kitas institucijas teisės aktų nustatyta tvarka.

2022 m. RRT karštąja linija gauti 1 523 pranešimai apie internete pastebėtą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją, iš jų pasitvirtino 694 pranešimai (253 pasikartojantys), o tolesnių veiksmų imtasi dėl 441 atvejo (tai sudaro 29 proc. visų gautų pranešimų). Palyginti su 2021 m., kai buvo gauti 3 558 pranešimai, matoma mažėjimo tendencija. Svarbu paminėti, kad RRT interneto karštąja linija gautų pranešimų skaičius nuolat kinta. 2022 m. gauta mažiau pranešimų apie vaikų seksualinio išnaudojimo vaizdus Lietuvos interneto erdvėje dėl to, kad 2021 m. buvo identifiкуotas Lietuvos informacijos prieglobos paslaugų teikėjas, per kurio serverius buvo aktyviai viešinama vaikų seksualinio išnaudojimo medžiaga, ir informacija pašalinta. Į RRT karštąją liniją kreipiasi tiek atsakingi piliečiai, tiek tarptautinės interneto karštųjų linijų asociacijos INHOPE tinklo nariai ir pateikia itin tikslius ir patikimus duomenis.

Ankstesniais metais RRT kovos su draudžiamu ir neigiamą poveikį nepilnamečiams darančiu turiniu internete sėkmė priklausė nuo to, kad interneto naudotojai RRT karštąja linija „**Švarus internetas**“ siuntė pranešimus, susijusius su pornografija, vaikų seksualiniu išnaudojimu, smurtu ir pan. RRT, siekdama efektyvinti draudžiamos informacijos aptikimo procesą, nuo 2022 m. pradžios naudoja bendradarbiaujant su „Oxylabs“ kompanija sukurtą inovatyvų, dirbtiniu intelektu grįstą sprendimą – automatinį paieškos įrankį, kuriuo ieško draudžiamo turinio Lietuvos interneto adresų (IP) erdvėje ir praneša RRT interneto karštajai linijai „**Švarus internetas**“.

10. Lietuvos policijos duomenimis, 2022 m. Lietuvoje registruoto nusikalstamumo augimą labiausiai nulėmė nusikalstamos veikos kibernetinėje erdvėje.

2022 m. šalies policijos įstaigose užregistruotos 42 988 nusikalstamos veikos, iš kurių 5 309 nusikalstamos veikos, arba 12 proc., padarytos kibernetinėje erdvėje. 2022 m. nusikalstamų veikų kibernetinėje erdvėje, palyginti su 2021 m., padaugėjo 2 775 atvejais, arba 52 proc.

Kaip ir pastaruosius kelerius metus, nusikalstamumą kibernetinėje erdvėje labiausiai nulėmė sukčiavimo (Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) 182 str.) atvejai, jie 2022 m. sudarė didžiąją – 48 proc. – dalį visų kibernetinėje erdvėje padarytų nusikalstamų veikų. Dominuojančių sukčiavimo būdų struktūra nesikeitė – išliko avansinio (išankstinio mokėjimo) sukčiavimo tendencija.

Lietuvos bankų asociacijos (toliau – LBA) duomenimis, finansiniai sukčiai iš Lietuvos gyventojų ir įmonių 2022 m. išviliojo beveik 12 mln. eurų¹¹. Tuo pačiu laikotarpiu finansų įstaigų bei teisėsaugos pastangomis savininkams buvo grąžinta apie 5 mln. eurų. Nors apgaule išviliotų lėšų suma didėjo palyginti nedaug (2021 m. išviliota 10,2 mln. eurų), užfiksuotų incidentų skaičius paaugo daugiau nei dvigubai. 2022 m., palyginti su 2021 m., nuo 3,5 tūkst. iki bemaž 8 tūkst. išaugo incidentų skaičius. Šie statistikos rodikliai rodo ne tik augantį sukčių aktyvumą, bet ir didesnę visuomenės atvirumą šia tema – nukentėjusieji drąsiau pasakoja apie savo patirtį, aktyviau praneša bankams apie patirtą arba gresiantį sukčiavimą, taip prisidėdami prie greitesnio nusikaltimo užkardymo. Lietuvos policijos duomenimis, 2022 m. didžiausią 457 142 eurų žalą patyrė Vilniaus draudimo bendrovė, kai buvo įsiterpta į elektroninį susirašinėjimą ir apgaulingai nurodyta banko sąskaita.



¹¹

LBA duomenys, <https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/finansiniai-sukciai-pemai-iviliojo-12-mln-euru-savininkams-grazinti-5-mln-euru>.

Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenimis (toliau – IRD prie LR VRM), 2022 m. šalyje užregistruota 919 elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų. (LR BK 196 – 198² str.), tai sudarė apie 2 proc. visų užregistruotų nusikaltimų veikų. 2021 m. šių nusikaltimų užregistruota 707, arba 212 mažiau (30 proc.).

Vis aiškiau matoma tendencija, kad nusikalstamas veikas Lietuvoje vykdančias asmenys veikia ne pavieniui, o gerai organizuotose grupėse, kurias identifikuoti, kaip ir tokio pobūdžio nusikalstamas veikas iširti, yra sudėtinga ir komplikuota dėl technologijų gausos, teisinių sunkumų, susijusių tiek su tokių veikų padarymo vietos nustatymu, tiek ir su ikiteisminiam tyrimui reikšmingų duomenų (informacijos) gavimu iš trečiųjų šalių. Nuo šių nusikaltimų veikų nukenčia ne tik Lietuvos, bet ir užsienio fiziniai ir juridiniai asmenys.

11. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) gaunamų pranešimų apie asmens duomenų saugumo pažeidimus (toliau – ADSP) sistemingai daugėja, tačiau tai siejama ne su pačių pažeidimų gausėjimu, o su duomenų valdytojų įgyjamų žinių, sąmoningumo asmens duomenų apsaugos srityje didėjimu.

VDAI gaunamų pranešimų apie ADSP kasmet daugėja (2018 m. – 100, 2019 m. – 175, 2020 m. – 181, 2021 m. – 239, 2022 m. – 304). VDAI pastebi, kad 2022 m., kaip ir anksčiau, nemažai ADSP sudarė duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *ransomware*). Duomenų valdytojais patyrė gana didelę žalą, turėjo šiems ADSP suvaldyti ir žalai bei poveikiui sumažinti skirti daug finansinių ir žmogiškųjų išteklių. Kiti asmens duomenų saugumo pažeidžiamumai buvo susiję su socialinės inžinerijos ir duomenų viliojimo metodais, tiekimo grandinės atakomis, prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragomis.

Pagal ADSP pobūdį Lietuvoje statistiškai neabejotinai vyrauja konfidencialumo pažeidimai, jų skaičius kasmet nuosekliai auga – 2022 m. net 269 atvejais (iš visų 304 registruotų) buvo prarastas asmens duomenų konfidencialumas.

Rusijos karas Ukrainoje sukėlė dar didesnę kibernetinių atakų bangą ir pablogino kibernetinio saugumo situaciją pasaulyje. Nors Rusijos karo kontekste VDAI specialių priemonių VDAI nerengė, tačiau dėl padidėjusios grėsmės organizacijų tvarkomiems asmens duomenims bendraudama su duomenų valdytojais ir tvarkytojais bei rengdama įvairias informuotumo skatinimo priemones pabrėžė būtinybę dar daugiau dėmesio skirti tinkamoms techninėms ir organizacinėms asmens duomenų tvarkymo priemonėms.

12. 2022-ieji informacinės konfrontacijos kontekste buvo išskirtiniai metai.

Bendras Lietuvai priešiškos informacinės veiklos atvejų skaičius 2022 m. iš viso sudarė 4 999 unikalios informacinius atvejus. Palyginti su pastarųjų penkerių metų duomenimis, 2022 m. informacinių incidentų skaičius išliko gana aukštas, nors informacinių atvejų, palyginti su 2021 m., ir mažėjo. Gynybos temų eskalacija 2022 m. išaugo beveik dvigubai: 2021 m. fiksuoti 26,42 proc. visų unikalų atvejų, o 2022 m. – 47,91 proc. Tai sutapo su reikšmingais užsienio ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti neigiamam šalies įvaizdžiui Vakaruose kurti ir Lietuvos visuomenės auditorijų tarpusavio susipriešinimui skatinti. Ypač daug dėmesio tiek Kremliaus, tiek Baltarusijos režimų kontroliuojami informacijos šaltiniai skyrė gynybos sektoriaus temoms: NATO, NATO pajėgumų stiprinimui Baltijos regione, Lietuvos

narystei NATO, Lietuvos karinio potencialo stiprinimui. Daug dėmesio taip pat sulaukė ir Lietuvos vykdoma užsienio politika: dvišaliai ir daugiašaliai santykiai, narystė tarptautinėse organizacijose, parama Ukrainai.

Politinių ir šalies saugumą stiprinančių procesų, kuriuose Lietuvos Respublika aktyviai dalyvavo arba kurie buvo tiesiogiai susiję su mūsų valstybe, gausa 2022 m. nulėmė ir didesnę neigiamą Rusijos bei Baltarusijos dėmesį Lietuvai. Priešiška informacinė veikla buvo susijusi su trimis strateginėmis sritimis: **(1) gynybos; (2) užsienio politikos** bei **(3) konstitucinių pagrindų apsaugos**.

2022 m. gynybos srities naratyvai daugiausia buvo skirti dezinformacijai apie NATO kaip instituciją, NATO ir Rusijos santykius skleisti. Jau 2021 m. pradėjęs agresyvėjantis Rusijos propagandinis tonas apie NATO kaip provokatorę ir neva blogėjančios pasaulio saugumo situacijos kaltininkę netilo ir 2022 m. tiesiogiai kaltinant JAV ir NATO dėl karo Ukrainoje pradžios.

2022 m. prieš Lietuvą ir valstybės institucijas įvykdyta mažiau priešiškų informacinių operacijų nei 2021 m. Sumažėjusių informacinių operacijų ir kibernetinių atakų prieš Lietuvos institucijas atvejų skaičių nulėmė Rusijos kibernetinių išpuolių prieš Ukrainos valstybines institucijas gausa.



03 Svarbiausi 2022 m. įvykiai kibernetinio saugumo srityje



ADSP – asmens duomenų pažeidimas
 AML – VŠĮ Pinigų plovimo prevencijos kompetencijų centras
 BDAR – Bendrasis duomenų apsaugos reglamentas
 DDoS – paslaugų trikdymo ataka (angl. Distributed Denial of Service)
 DOMREG – interneto paslaugų centras
 FNTT – Finansinių nusikaltimų tyrimo tarnyba
 KAM – Krašto apsaugos ministerija
 LR VRM – Lietuvos Respublikos vidaus reikalų ministerija
 NKSC – Nacionalinis kibernetinis saugumo centras

04

Pagrindiniai ataskaitoje
vartojami terminai ir sąvokos1 Pagrindiniai
ataskaitoje vartojami
terminai ir sąvokos

1. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.
2. **„Botnet“ tinklas** – tinklas, kuris sudaromas užkrėtus daug kompiuterių ir vėliau juos panaudojant įvairioms, dažniausiai DDoS, atakoms vykdyti
3. **Didelio poveikio kibernetinis incidentas** – tai kibernetinis incidentas, kurio poveikis atitinka du ir daugiau kriterijų: ryšių ir informacinė sistema (toliau – RIS) trukdoma ≥ 2 val., paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000 , arba 25 proc., paslauga trikdoma visos šalies teritorijos ir (ar) ≥ 1 ES šalyje, pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas, nuostoliai $\geq 500\,000$ eurų.
4. **Draudžiama skleisti informacija** – viešoji informacija, kuri pagal Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymą yra priskirtina draudžiamai skleisti informacijai, tai yra kuria iš vaikų ar kitų asmenų tyčiojamasi arba jie niekinami dėl tautybės, rasės, lyties, kilmės, neįgalumo, seksualinės orientacijos, socialinės padėties, kalbos, tikėjimo, įsitikinimų, pažiūrų ar kitais panašiais pagrindais arba kuri yra pornografinio turinio, skatina vaikų seksualinę prievartą, jų išnaudojimą, pateikia savitikslių smurtą ir (ar) yra kitais įstatymais draudžiama viešoji informacija⁰¹.
5. **Informacinė ataka** – dezinformacija, propaganda ir kita kryptinga informacijos sklaida, nukreipta prieš Lietuvos nacionalinio saugumo interesus⁰².
6. **Informacinis incidentas** – vienkartinis ne ES ir (ar) NATO valstybių narių ar jų subjektų informacinis veiksmas, kuriuo, tendencingai informuojant visuomenę, siekiama paveikti su Lietuvos Respublikos nacionalinio saugumo interesais susijusių sprendimų priėmimo procesą ir kuris tiesiogiai nėra susijęs su kitais tokiais veiksmais⁰³.
7. **Informacinė operacija** – suplanuoti ir koordinuoti veiksmai bei priemonės, siekiant daryti įtaką norimai auditorijai.
8. **Informacinis raštingumas** apima gebėjimą identifikuoti, gauti, vertinti, atrinkti ir etišškai bei atsakingai naudoti reikalingą informaciją iš įvairių informacijos šaltinių.
9. **Informacinis spaudimas** – ne ES ir (ar) NATO valstybių narių ar jų subjektų tęstiniai (nuolat pasikartojantys, su kitais informaciniais incidentais tiesiogiai susiję veiksmai) informaciniai incidentai ar jų visuma, siekiant visuomenės informavimo priemonėmis paveikti su Lietuvos Respublikos nacionalinio saugumo interesais susijusių sprendimų priėmimo procesą (žr. pav. 1⁰⁴).

01

Pagal Lietuvos Respublikos švietimo įstatymo 23² straipsnio 2 dalies 1 punktą.

02

Lietuvos karinė doktrina (2016), https://kariuomene.kam.lt/lt/kariuomenes_atributika/lietuvos_karine_doktrina.html.

03

Pagal Strateginės komunikacijos nacionalinio saugumo srityje koordinavimo tvarkos aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2020 m. rugpjūčio 26 d. nutarimu Nr. 955.

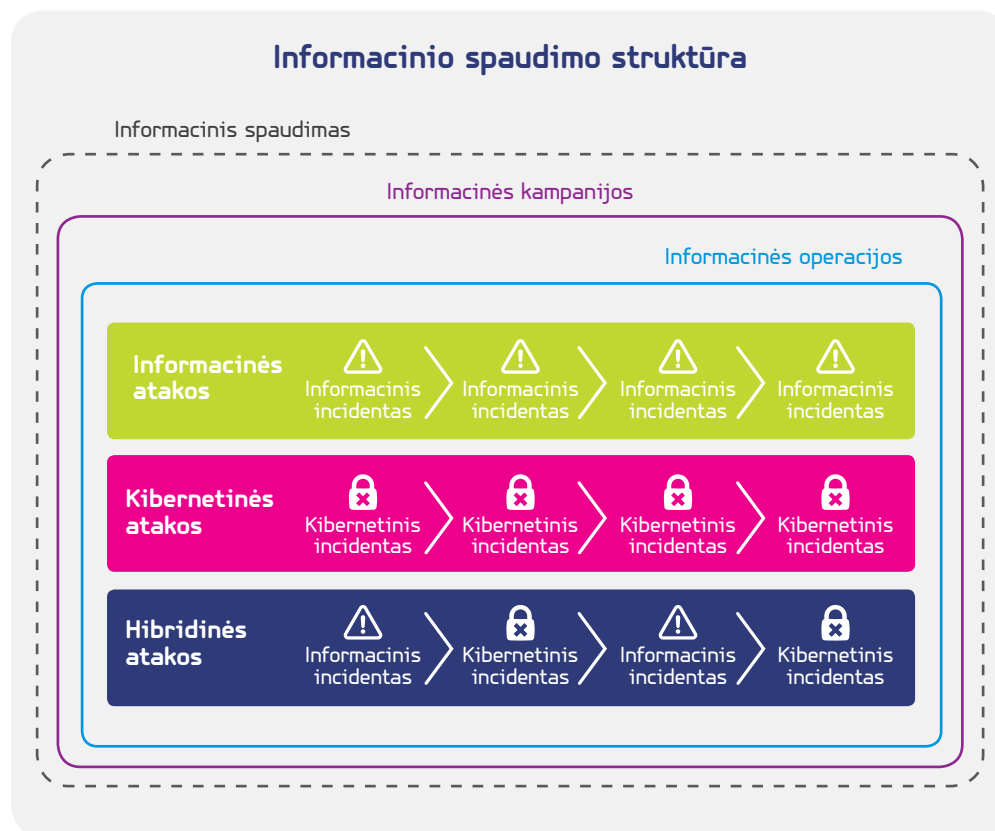
04

Ten pat.



1 pav. >

Informacinio
spaudimo struktūra
(šaltinis – Lietuvos
kariuomenės Strateginės
komunikacijos
departamentas (LK SKD))



- 10. Ypatingos svarbos informacinė infrastruktūra** – RIS ar jos dalis, RIS grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.
- 11. Hibridinė ataka** – kibernetinis incidentas kartu su informaciniu incidentu.
- 12. Kibernetinė ataka** – elektroninėje aplinkoje pavienių asmenų arba organizacijų vykdomas informacinių sistemų, infrastruktūros objektų, kompiuterių tinklų, asmeninių kompiuterių bei telefonų puolimas kenkimo programomis.
- 13. Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį RIS perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdančios ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą⁰⁵.
- 14. Kibernetinio saugumo informacinis tinklas** – valstybės informacinė sistema, kurios paskirtis – informacinių technologijų priemonėmis tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus, keistis informacija apie galimus ir įvykusius kibernetinius incidentus Kibernetinio saugumo įstatymo 13 str. 4 dalyje nustatytais atvejais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija.
- 15. Kibernetinio saugumo subjektas** – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

05

Lietuvos Respublikos kibernetinio saugumo 2018 m. birželio 27 d. įstatymo Nr. XII-1428 pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lit/TAD/15e540727ac211e89188e-16a6495e98c>.

- 16. Konstitucinių pagrindų apsaugos sektorius** – tai Lietuvos konstitucinės santvarkos pagrindai ir apsauga, pamatiniai Lietuvos valstybės principai: valstybės nepriklausomybė, tautos suverenitetas ir demokratija, valdymo forma, valstybės teritorijos vientisumas, teisinė valstybė, asmens teisių ir laisvių apsauga.
- 17. Nereikšmingo poveikio kibernetinis incidentas** – tai kibernetinis incidentas, kurio poveikis atitinka bent vieną iš kriterijų: RIS trikdoma < 1 val., paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 proc., paslauga teikiama, bet trikdoma, nuostoliai < 250 000 eurų.
- 18. Nepakeičiamas žetonas** (angl. *non-fungible token*, NFT) – unikalūs ir nepakeičiamas duomenų vienetas, laikomas blokų grandinėje. NFT – sertifikatas, patvirtinantis tam tikro skaitmeninio vieneto autentiškumą.
- 19. Nusikaltimai kibernetinėje erdvėje plačiąja prasme** – bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo panaudotos informacinės ir ryšių technologijos, o nusikaltimo faktui įrodyti turi būti taikomos specifinės nusikaltimų kibernetinėje erdvėje tyrimo priemonės.
- 20. Nusikaltimai kibernetinėje erdvėje siaurąja prasme** – nusikaltimai, tiesiogiai darantys įtaką elektroninių duomenų ir informacinių sistemų saugumui, kitaip tariant, pati informacinė sistema yra nusikaltimo tikslas.
- 21. Padidinto tarifo paslauga** – paslauga, išskyrus trumpuoju numeriu 118 teikiamas informacijos paslaugas, kurios tarifas nėra tiksliai nurodytas abonentų pasirinktame mokėjimo plane ir yra didesnis už nacionalinių skambučių ir trumpųjų žinučių (SMS) bei vaizdo žinučių (MMS) paslaugų teikimo tarifus⁰⁶.
- 22. Perkeltieji asmenys** – žmonės, kurie valstybės įstatymų ar kita nustatyta tvarka dėl įvairių priežasčių (ekonominių, rečiau politinių ar socialinių) perkeltami iš vienos gyvenamosios vietos į kitą.
- 23. Unikalus informacinis atvejis** – pirminis, faktologinis, autorinis ar kitoks informacinės sklaidos atvejis, kuriame ryškūs dezinformacijos, manipuliacijos, klaidinančios informacijos ar kitos apgaulės technikos bruožai. Unikalių atvejų pasidalijimai kituose informacijos kanaluose ar socialiniuose tinkluose neskaičiuojami, todėl vertinant auditorijų pasiekiamumą reikėtų turėti omeny ir pasidalijimų efektą⁰⁷.
- 24. Vidutinio poveikio kibernetinis incidentas** – tai kibernetinis incidentas, kurio poveikis atitinka du ir daugiau kriterijų: RIS trukdoma ≥1 val., bet <2 val., paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <1000, arba 25 proc., paslauga trikdoma dalyje šalies teritorijos, pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas, nuostoliai ≥250 000, bet <500 000 eurų.



06

Pagal Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2005 m. gruodžio 13 d. įsakymu Nr. 1V-1104 patvirtintų Telefono ryšio numerių skyrimo ir naudojimo taisyklių 7 punktą.

07

LK SKD Informacinės aplinkos vertinimo skyriaus nustatytas terminas.

05

Kibernetinio saugumo aplinkos stiprinimas



Greta Monika Tučkutė,
krašto apsaugos viceministrė

Vadovo žodis

Kibernetiniam saugumui Lietuvoje, taip pat ir kitose Europos Sąjungos šalyse, skiriame vis daugiau dėmesio: priimami nauji teisės aktai, atnaujinami kibernetinio saugumo srities standartai, organizuojama nemažai renginių ir mokymų kibernetinio saugumo temomis, o viešojoje erdvėje kibernetinis saugumas yra viena aktualių pastarojo meto temų. Ypač šiai sričiai dėmesio padaugėjo Rusijai pradėjus karą Ukrainoje, nes dar labiau išryškėjo poreikis stiprinti Lietuvos kibernetinį atsparumą ir kiekvieno iš mūsų gebėjimus apsisaugoti, atremti kibernetines grėsmes ar kuo skubiau atsikurti po įvykusio kibernetinio incidento.

Kibernetinio saugumo politikos formavimo klausimai yra Krašto apsaugos ministerijos veiklos prioritetų sąraše bei įtvirtinti Vyriausybės programoje, tad nuosekliai juos įgyvendiname. Noriu pasidžiaugti pažanga, kurią padarėme užtikrindami tiekimo grandinės saugumą, stiprindami kritinę infrastruktūrą, vienydami bendraminčius Europoje. Šiuo metu vyksta intensyvūs NIS2 direktyvos, kurios įgyvendinimas Lietuvoje prisidės prie aukštesnio visos Europos kibernetinio saugumo lygio, nuostatų perkėlimo darbai.



KĄ SAUGO?

- ✓ Lietuvos interesus atitinkančią tarptautinę ir vidaus saugumo sistemą.



NUO KO SAUGO?

- ✓ Visuomenės ir valstybės atsparumą trikdančių išorės ir vidaus grėsmių.



KAIP SAUGO?

- ✓ Rengdama teisės aktus, susijusius su kibernetinio saugumo užtikrinimu.
- ✓ Kartu su strateginiais partneriais dalyvaudama bendruose projektuose dėl reagavimo į kibernetines atakas ir jų užkardymo.
- ✓ Stiprindama nacionalinius kibernetinio saugumo pajėgumus ir valstybės informacinius išteklius.
- ✓ Atstovaudama Lietuvai tarptautiniuose kibernetinio saugumo politikos formatuose.
- ✓ Skatindama kibernetinio saugumo inovacijas ir mokslinę veiklą.



KRAŠTO APSAUGOS
MINISTERIJA



NKC
NACIONALINIS
KOORDINAVIMO CENTRAS
LIETUVA

Reikšmingiausi KAM 2022 m. vykdyti darbai kibernetinio saugumo politikos formavimo srityje, nuveikti stiprinant ne tik Lietuvos kibernetinės erdvės saugumą, bet ir prisidedant prie tarptautinio saugumo ir euroatlantinių vertybių plėtros. Išskirtinis praėjusių metų įvykis – Lietuvos kaimynystėje prasidėjęs Rusijos karas prieš Ukrainą, palietęs ir kibernetinio saugumo sritį.

1 ES gynybos iniciatyvų panaudojimas bendradarbiavimui

Parama Ukrainai

Nuo pat 2022 m. pradžios kibernetinės atakos buvo neatsiejama Rusijos karinės agresijos prieš Ukrainą dalis. Atakos turėjo poveikį ne tik Ukrainai, bet ir kitoms ES ir NATO valstybėms. ES kibernetinė darbo tvarkė 2022 m. koncentruota į ES ir atskirų ES valstybių narių visapusiškos paramos Ukrainai teikimą ir ES teisėkūros pasiūlymų kibernetinio saugumo srityje derinimą. Per 2022 m. Lietuva kartu su kitomis ES valstybėmis narėmis aktyviai teikė Ukrainai kibernetinio saugumo paramą, įskaitant įrangos ir programinės įrangos teikimą.

ES Kibernetinės greitojo reagavimo pajėgos

Lietuva nuo 2018 m. koordinuoja ES nuolatinio struktūrizuoto bendradarbiavimo projektą „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (toliau – PESCO projektas), kuriame dalyvauja aštuonių ES valstybių: Estijos, Belgijos, Kroatijos, Lenkijos, Lietuvos, Nyderlandų, Rumunijos ir Slovėnijos⁰¹, atstovai. PESCO projekto tikslas – užkirsti kelią kibernetinėms atakoms ir reaguoti į kibernetinius incidentus ES valstybėse narėse, dalyvauti bendros saugumo ir gynybos politikos karinėse misijose ir operacijose bei teikti paramą partneriams.

Lietuva, Nyderlandai, Lenkija, Estija, Rumunija ir Kroatija 2022 m. vasario 22 d. aktyvavo ES Kibernetinės greitojo reagavimo pajėgas, reaguodamos į Ukrainos užsienio reikalų ministro Dmytro Kulebos 2022 m. vasario 18 d. kreipimąsi į ES institucijų ir valstybių narių atstovus su kibernetinės paramos prašymu. ES Kibernetinės greitojo reagavimo pajėgos teikė paramą 2022 m. lapkričio mėn. Moldovoje ir atliko pažeidžiamumų vertinimą⁰².

2022 m. ES Kibernetinių greitojo reagavimo pajėgų atstovai dalyvavo kibernetinio saugumo pratybose Lietuvoje „Gintarinė migla 2022“, mokymuose ir pratybose Rumunijoje bei pratybose „CyberNet22“ Nyderlanduose, čia užėmė antrąją vietą.

01

Slovėnija ir Belgija projekto dalyvėmis tapo 2023 m. kovo 8 d., <https://kam.lt/belgija-ir-slovenija-jungiasi-prie-lietuvos-vadovaujamo-es-kibernetiniu-greitojo-reagavimo-pajegu/>.

02

2023 m. kovo mėn. ES Kibernetinės greitojo reagavimo pajėgos teikė paramą ES karinėje misijoje Mozambique, ten taip pat buvo atliktas pažeidžiamumų vertinimas, <https://kam.lt/lietuvas-vadovaujamos-es-kibernetines-greitojo-reagavimo-pajegos-atsakas-i-incidentus-tiek-es-viduje-tiek-remiant-es-partnerius-ir-karines-misijas/>.



2 KAM veikla plėtojant bendradarbiavimą su strateginiais sąjungininkais ir partneriais Europoje

Bendradarbiavimas su JAV

2021–2022 m. Lietuva dalyvavo JAV kuruojamoje tarptautinėje iniciatyvoje prieš išpirkos reikalaujančias atakas (angl. *Counter Ransomware Initiative*), kurios tikslas – suvienyti 36 šalių pastangas kovojant su Rusijos ir kitų šalių organizuojamomis išpirkomis reikalaujančiomis atakomis, stiprinti tinklų atsparumą ir griauti nusikalstamų grupuočių infrastruktūrą. Projekte Lietuva kartu su Indija koordinavo kibernetinio atsparumo darbo grupę ir su partneriais vystė nuolatinę struktūros „International Counter Ransomware Task Force“ koncepciją, prisidėdiančią prie projekto galimybių dar geriau analizuoti įvykusius incidentus ir apsaugoti nuo išpirkos reikalaujančių atakų.

KAM įsteigtas NKC

NKC įsteigtas KAM 2022 m. pradžioje pagal 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentą (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas⁰³. Būtent šio tinklo sudedamąja dalimi tampa KAM veikiantis NKC, kurio funkcijos apims kibernetinio saugumo bendruomenės kūrimą ir informavimą, kibernetinio saugumo švietimo sklaidą, ES strateginių dokumentų kibernetinio saugumo srityje įgyvendinimą. NKC talkina partneriai: NKSC, VŠĮ Inovacijų agentūra bei VŠĮ Centrinė projektų valdymo agentūra. Naudodamas „Skaitmeninės Europos“ programos bei KAM biudžeto lėšas, 2023 m. pab. NKC skelbs kvietimus MVĮ projektų kibernetinio saugumo inovacijų srityse finansavimui iki 60 tūkst. eurų gauti (pavyzdžiui, kibernetinio saugumo sprendimams „EdTech“ srityje ir kibernetinio saugumo sprendimams MVĮ atsparumui didinti). Lietuvos NKC taip pat vykdys kitas visiems ES šalyse veikiantiems NKC būdingas veiklas, tokias kaip kibernetinio saugumo kultūros kėlimas ar dalijimasis kibernetinio saugumo žiniomis.

Dalyvavimas formuojant ir įgyvendinant ES bendrą saugumo ir gynybos politiką

Dar iki Rusijos karo Ukrainoje pradžios 2022 m. sausio–vasario mėn. ES Taryboje surengtos didelio masto ES kibernetinės krizės pratybos „EU-CyCLEs“. Pratybose buvo tobulinamas gebėjimas ES reaguoti į didelio masto kibernetinius incidentus ir atakas bei gerintas suvokimas dėl galimo ES sutarties 42.7 straipsnio (tarpusavio pagalbos) aktyvavimo, taip pat testuoti turimi ES mechanizmai. KAM 2022 m. lapkričio 7 d. Lietuvoje kartu su ES Tarybai pirmininkaujančios Čekijos ir ENISA atstovais surengė kasmetines krizių valdymo pratybas „BlueOLEX 2022“. Pratybos skirtos Europos ryšių palaikymo Kibernetinių krizių organizacinio tinklo (angl. *Cyber Crisis Liaison Organisation Network (CyCLONE)*) operacinėms veikimo procedūroms testuoti ir tobulinti. „CyCLONE“ pratybos padeda visai ES geriau pasirengti bendram didelio masto kibernetinių incidentų ir krizių valdymui. 2022 m. Vilniuje vykusiose pratybose dalyvavo atstovai iš 22 ES valstybių narių, taip pat iš Europos Komisijos ir ENISA. Siekiant gerinti tarpusavio bendradarbiavimą krizės atveju, 2022 m. pirmą kartą į pratybų scenarijų įtrauktos ne tik ES valstybės narės, bet ir ES institucijos, įstaigos ir agentūros. Pastarųjų pratybų paraštėse vykusioje neeilinėje Lietuvos Kibernetinio saugumo tarybos bei Europos Komisijos ir ENISA sesijoje aptartos nacionalinės ir ES lygmens kibernetinio saugumo iniciatyvos ir prioritetai.



03

2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas, <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32021R0887>.



ES teisėkūros iniciatyvos

Podvejus metus trukusių derybų 2022 m. gruodžio 27 d. oficialiajame ES leidinyje paskelbta NIS2 direktyva⁰⁴, kuri sustiprins viešojo ir privataus sektoriaus bei visos ES kibernetinį atsparumą ir reagavimo į incidentus pajėgumus. NIS2 direktyva įsigaliojo 2023 m. sausio 16 d., šio ES teisės akto nuostatomis perkelti valstybėms narėms skirtas 21 mėnuo. KAM, bendradarbiaudama su kitomis suinteresuotomis Lietuvos institucijomis ir organizacijomis, derybose išlaikė ambicingus NIS2 direktyvos tikslus dėl taikymo srities išplėtimo, aukštesnio lygio rizikos valdymo ir aiškių kriterijų nustatymo, kartu užtikrinant šių nuostatų proporcingumą.

Šiuo metu atliekamas NIS2 direktyvos nuostatų ir jų atitikties teisės aktams vertinimas, jų aptarimas su susijusiomis Lietuvos institucijomis. Preliminariai nustatyta, kad dėl įsigaliojusios NIS2 direktyvos gali reikėti keisti 11 teisės aktų ir įtraukti kitas institucijas (pagal kompetencijas elektroninių ryšių, asmens duomenų apsaugos, krizių valdymo, finansų sektoriaus srityje ir pan.).

ES Taryba 2022 m. lapkričio 18 d. pritarė pasiūlymui sukurti bendrą kibernetinio saugumo taisyklių rinkinį visoms ES institucijoms. Lietuva kartu su dauguma kitų ES valstybių narių derybose siekė, kad ES institucijoms būtų taikomi aukšti kibernetinio saugumo reikalavimai ir standartai, atitinkantys ES valstybėms narėms taikomas nuostatas pagal NIS2 direktyvą.

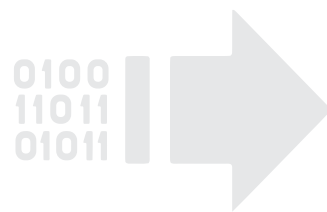
2022 m. rugsėjo 15 d. Europos Komisija pateikė naują ES reglamento pasiūlymą dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, vadinamąjį Kibernetinio atsparumo aktu. Teisės aktu siekiama nustatyti horizontaliuosius privalomus kibernetinio saugumo reikalavimus techninės ir programinės įrangos produktams visam jų gyvavimo ciklui. Lietuva, kaip ir kitos ES valstybės, sutinka, kad į ES rinką patektų tik aukščiausius atsparumo, apsaugos ir saugumo standartus atitinkančios technologijos, o prasidėjusiose ES Tarybos derybose tikslinamos teisės akto pasiūlymo nuostatos.

2022 m. gegužės 23 d. priimtos ES Tarybos išvados dėl ES kibernetinės pozicijos vystymo. Išvados mis demonstruojamas ES pasiryžimas nedelsiant ir ilgalaikėmis priemonėmis reaguoti į esamas ir kylančias kibernetines grėsmes ir veikėjus, siekiančius daryti poveikį ES strateginiams interesams, įskaitant ir partnerių saugumą.

ES Taryba 2022 m. spalio 17 d. patvirtino Tarybos išvadas dėl informacinių ir ryšių technologijų (IRT) tiekimo grandinių saugumo. Tiekimo grandinės saugumo užtikrinimas Lietuvai yra ypatingos reikšmės klausimas, todėl ji tiesiogiai dalyvavo rengiant ES lygmens politinių gairių projektą. Lietuva taip pat per pastaruosius metus įvairaus formato ES kibernetinio saugumo susitikimuose dalijosi patirtimi priimant nacionalinius teisės aktus, kuriais siekiama suvaldyti dėl nepatikimos IRT įrangos ar paslaugų naudojimo kylančias rizikas nacionaliniam saugumui.

04

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



ES kibernetinė diplomacija

Rusijos karo prieš Ukrainą kontekste ES ir ES valstybės narės deklaracijomis griežtai pasmerkė vykdomas kibernetines atakas: 2022 m. sausio 14 d. paskelbta ES deklaracija, smerkianti sausio 13 ir 14 d. kibernetines atakas prieš Ukrainos vyriausybinius tinklus⁰⁵, o 2022 m. gegužės 10 d. ES pirmą kartą istorijoje viešai priskyrė Rusijai kibernetinę ataką prieš palydovinį tinklą KA-SAT⁰⁶.

Lietuvos iniciatyva 2022 m. liepos 19 d. paskelbta bendra ES deklaracija dėl prieš Lietuvą ir kitas Europos šalis nukreiptų prorusiškų kibernetinių programiškų atakų Rusijos karo Ukrainoje kontekste.

Siekdama atgrasyti iš trečiųjų šalių ar nusikalstamų veikėjų kylančias kibernetines grėsmes ir atakas ES ir ES valstybėms narėms, ES Taryba 2022 m. gegužę pratęsė kibernetinių ribojamųjų priemonių sistemos galiojimą dar trejiems metams – iki 2025 m. gegužės 18 d. Pagal šią sistemą ES gali taikyti tikslines ribojamąsias priemones su kibernetiniais išpuoliais susijusiems asmenims ar subjektams, kurie daro didelį poveikį ir kelia išorės grėsmę ES ar jos valstybėms narėms. Šiuo metu kibernetinių sankcijų sąrašė yra aštuoni asmenys ir keturi subjektai iš Rusijos, Kinijos ir Šiaurės Korėjos.

ES kibernetinės diplomatijos sistema taip pat apima bendradarbiavimą stiprinančias priemones, pagal kurias per 2022 d. surengti ES ir Ukrainos bei ES ir JAV kibernetiniai dialogai.

ES kibernetinė gynyba

2022 m. lapkričio 10 d. Europos išorės veiksmų tarnyba ir Europos Komisija paskelbė komunikatą⁰⁷ dėl ES kibernetinės gynybos politikos, kuria siekiama stiprinti ES kibernetinės gynybos pajėgumus, karinių bei civilinių kibernetinių bendruomenių veiklos koordinavimą ir jų tarpusavio bendradarbiavimą. Reaguodama į paskelbtą komunikatą, ES Taryba numato per 2023 m. patvirtinti Tarybos išvadas ir veiksmų planą.

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

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

Nuo 2022 m. balandžio mėn. įsigaliojo teisės aktai, užtikrinantys, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga. Priimti Lietuvos Respublikos viešųjų pirkimų įstatymo⁰⁸, Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo⁰⁹, Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymo¹⁰ pakeitimai, kuriais siekiama valdyti rizikas, kylančias nacionaliniam saugumui dėl nesaugių (nepatikimų) informacinių technologijų naudojimo kritinėje valstybės infrastruktūroje.

05

Vyriausiojo įgaliotinio deklaracija ES vardu dėl kibernetinio išpuolio prieš Ukrainą, <https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/>.

06

Rusijos kibernetinės operacijos prieš Ukrainą. Vyriausiojo įgaliotinio deklaracija ES vardu, <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>.

07

Kibernetinė gynyba. ES stiprina kovą su kibernetinėmis grėsmėmis, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642.

08

Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 25, 27, 35, 37, 39, 45, 47, 51, 90 ir 92 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/0ed02bd3a5ff11ecaf79c2120caf5094?positionInSearchResults=1&searchModelUUID=90d1a3c6-7c67-4c0e-8293-f08f9cb05fd0>.

09

Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo Nr. XIII-328 2, 29, 37, 39, 48, 50, 52, 58, 98 ir 100 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/409b3602a5ff11ecaf79c2120caf5094?positionInSearchResults=0&searchModelUUID=c763dc84-b132-4afa-ac32-baad3018a0f2>.

10

Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymo Nr. XI-1491 4, 6, 17, 24, 33, 34, 40, 44 ir 54 straipsnių pakeitimo įstatymas, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/83c76892a5ff11ecaf79c2120caf5094>.

2022 m. tęstas 2021 m. pradėtos Programos rengimas, į jos įgyvendinimą įtraukiamos įvairios valstybės institucijos. Šiame etape buvo analizuojama problematika ir sprendimai.

Nacionalinės kibernetinio saugumo plėtros programos kryptys



Stiprinti viešojo sektoriaus subjektų ir strateginių valstybės įmonių kibernetinio saugumo infrastruktūrą.



Efektyvinti kovą su nusikaltimais elektroninėje erdvėje ir didinti jų prevenciją.



Gerinti kompetencijas bei edukaciją kibernetinio saugumo srityje.



Vystyti viešojo ir privataus sektorių partnerystės iniciatyvas.



Stiprinti tarptautinį bendradarbiavimą.

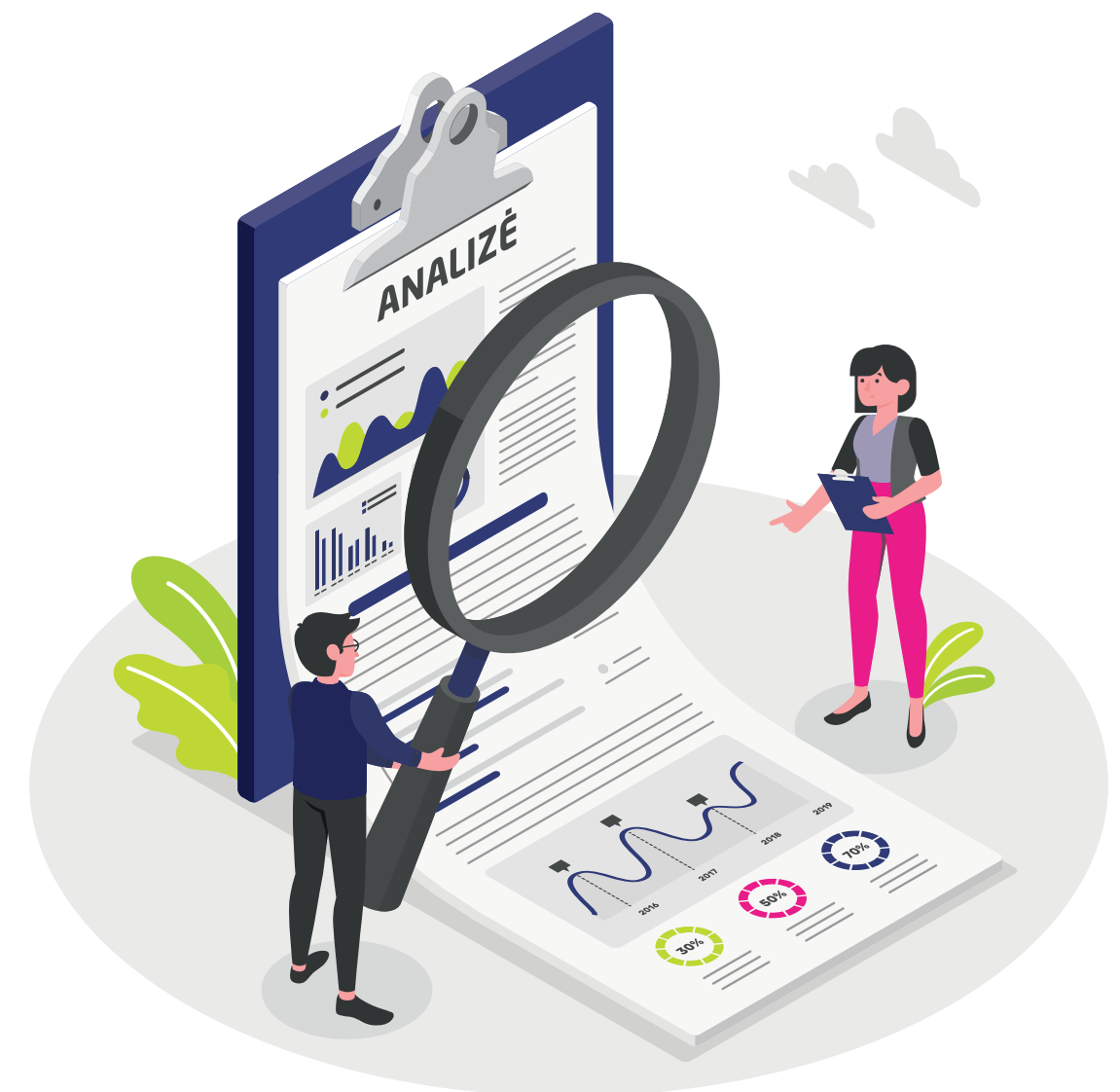
2022 m. susitikimuose su įvairiomis valstybės institucijomis atlikta kibernetinio saugumo problematikos analizė bei aptartos Programos finansavimo galimybės. Planuojama dalį Programos veiklų finansuoti Ekonomikos gaivinimo ir atsparumo didinimo plano „Naujos kartos Lietuva“ lėšomis ir skirti 40,15 mln. eurų.

KAM dalyvavo rengiant valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo ES valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) NATO valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašą¹¹. Šis tvarkos aprašas nustato Lietuvos Respublikos Vyriausybės įgaliotos institucijos ir į Vyriausybės nutarimu patvirtintą sąrašą įtrauktų registrų ir valstybės informacinių sistemų valdytojų ir šių sistemų tvarkytojų veiksmus, siekiant užtikrinti, kad valstybės informaciniai ištekliai būtų prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, ir taip garantuoti jų apsaugą.

KAM ir toliau aktyviai siekia sustiprinti perkančiųjų organizacijų tiekimo grandinės saugumą, todėl nuo 2020 m. vykdė ypatingos svarbos informacinės infrastruktūros valdytojų sandorių vertinimą. KAM vertina, ar perkančiosios organizacijos pirkimo medžiagoje nustato kibernetinio saugumo reikalavimus, informacijos saugos politikos reikalavimus tiekėjui ir su pirkimo objektu susijusioms paslaugoms, ir atitinkamai rekomenduoja valdyti nustatytas technologines rizikas.

11

Valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2022 m. liepos 11 d. nutarimu Nr.739, <https://www.e-tar.lt/portal/lt/legalAct/8d0f9bd001a711ed8fa7d02a65c371ad>.



06

Lietuvos kibernetinio saugumo būklės apžvalga



Kibernetinių incidentų ir jų valdymo situacijos Lietuvoje apžvalga



Liudas Ališauskas,
NKSC direktorius

Vadovo žodis

2022 m. Nacionalinis kibernetinio saugumo centras daug dėmesio skyrė savo tęstiniam uždaviniui – stiprinti mūsų šalies kibernetinį atsparumą. Konsultavome Lietuvos kritinės infrastruktūros valdytojus dėl efektyvaus kibernetinio saugumo priemonių taikymo, karo Ukrainoje kontekste pabrėžiame būtinybę turėti pajėgumus, kurie leistų jiems atkurti teikiamas kritines paslaugas ir užtikrinti veiklos tęstinumą. Tęsėme kibernetinio saugumo mokymus viešojo sektoriaus darbuotojams. Įdiegėme ir pradėjome naudoti modernų virtualų kibernetinės gynybos poligoną, šiuo metu jame treniruojame ir ugdome įvairius kibernetinio saugumo specialistus. Visos šios priemonės leido šalyje išlaikyti stabilią kibernetinio saugumo situaciją bei didinti bendrą atsparumo lygį. 2023 m. ir toliau bus daug dėmesio skiriama kibernetinio saugumo subjektų atsparumui, efektyvesniam kibernetinių incidentų valdymui ir bendradarbiavimui su kitomis kibernetinius incidentus valdančiomis institucijomis stiprinimui siekiant efektyvesnės nacionalinės kibernetinės gynybos architektūros.



KĄ SAUGO?

- ✓ Lietuvos kibernetinę erdvę ir kibernetinio saugumo subjektus.



NUO KO SAUGO?

- ✓ Nuo kibernetinių incidentų ir jų neigiamo poveikio.



KAIP SAUGO?

- ✓ Atlikdamas kibernetinių incidentų valdymą ir analizę (CERT-LT).
- ✓ Vykdydamas tyrimus, pratybas ir švietimą kibernetinio saugumo klausimais.
- ✓ Užtikrindamas KAS valdomų ryšių ir informacinių sistemų kibernetinį saugumą.
- ✓ Atlikdamas Nacionalinės komunikacijų apsaugos ir Saugumo priežiūros tarnybų funkcijas; nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas.
- ✓ Atlikdamas informacinių išteklių ir kibernetinio saugumo subjektų atitikties teisės aktų nustatytiems kibernetinio saugumo ir elektroninės informacijos saugos reikalavimams vertinimo, priežiūros ir stebėsenos funkcijas.
- ✓ Koordinuodamas kibernetinio saugumo subjektų RIS spragų atsakingą atskleidimą.
- ✓ Plėtodamas tarptautinį bendradarbiavimą kibernetinio saugumo srityje.



NACIONALINIS
KIBERNETINIO SAUGUMO
CENTRAS

1 Fiksuotų kibernetinių incidentų dinamika Lietuvoje

2022 m. NKSC CERT-LT iš viso užregistravo 4 080 kibernetinių incidentų, jų skaičius išliko panašus, kaip ir 2021 m.⁰¹ (1 pav.).

1 pav. >

2019–2022 m. NKSC fiksuotų kibernetinių incidentų statistika (šaltinis – NKSC)

Metai	Iš viso	Nereikšmingo poveikio	Vidutinio poveikio	Didelio poveikio
2022	4080	4047	33	0
2021	4088	3995	93	0
2020	4330	4262	67	1
2019	3241	N/D	N/D	N/D

Iš visų 2022 m. fiksuotų incidentų 33 priklauso vidutinei kategorijai. Šios kategorijos incidentai dažniausiai buvo susiję su DDoS atakomis, kenksmingo programinio kodo, skirto prieigai prie ryšių informacinių sistemų gauti ir kenkimo veiklai vykdyti (pavyzdžiui, šnipinėjimą ir kitus destruktivius veiksmus), platinimu. Taip pat fiksuota su modernia kenkimo programine įranga (angl. *advanced persistent threat*, APT) siejama valstybinių veikėjų veikla (2 pav.).

2 pav. >

CERT-LT 2022 m. fiksuotų vidutinės kategorijos incidentų pasiskirstymas pagal kibernetinių incidentų grupes (šaltinis – NKSC)

Vidutinės kategorijos kibernetinių incidentų grupės	2022 m.
DDoS atakos	9
Neteisėta prieiga prie RIS, programinės įrangos	5
Teikiamų paslaugų nutraukimas	5
Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai	4
Moderni kenkimo programinė įranga	3
Kita	7

Palyginti su ankstesniais metais, vidutinės kategorijos incidentų skaičius sumažėjo 35 proc. (2021 m. – 93 atvejai). Mažėjimo priežastys susijusios su NKSC veiksmiais metų pradžioje – subjektai buvo aktyviai informuojami ir jiems teikiami nurodymai dėl prevencinių apsaugos priemonių, taip pat su išaugusiu subjektų dėmesiu kibernetiniam saugumui. Kita vertus, 2021 m. vidutinės kategorijos incidentų skaičiaus augimą lėmė tais metais identifiukuoti plačiai naudojamų programų „MS Exchange“, „Log4j“, kt. „nulinės dienos“ (angl. *zero day*) pažeidžiamumai ir jų išnaudojimas Lietuvoje.

01

NKSC pateikiama kibernetinių incidentų statistika remiasi CERT-LT gautais pranešimais. Remiantis įstatymais, priverolę pranešti apie patirtus kibernetinius incidentus turi tik kibernetinio saugumo subjektai, o didelė dalis verslo įmonių ir privatūs asmenys tai gali padaryti savanoriškai, todėl realus Lietuvoje vykstančių kibernetinių incidentų skaičius didesnis, negu pateikiama šioje ataskaitoje.

Apžvelgiant 2022 m. NKSC užfiksuotus kibernetinius incidentus, kaip ir prieš metus, daugiausia incidentų buvo susiję su kenkimo programinės įrangos platinimu, socialinės inžinerijos atakomis, kuriomis siekta išvilioti įvairius jautrius duomenis (angl. *phishing*), nepageidaujamos informacijos platinimu, mėginimais įsilaužti. Tačiau, priešingai negu ankstesniais metais, išaugo DDoS atakų skaičius (3 pav.).

02

Patarimai, kaip apsisaugoti nuo sukčių kibernetinėje erdvėje, kurie bando pasinaudoti karo Ukrainoje situacija, NKSC, https://www.nksc.lt/naujienos/patarimai_kaip_apsisaugoti_nuo_sukciu_kibernetinej.html.

Nr.	Kibernetinio incidento grupės	2022 m. skaičius	2021 m. skaičius	Pokytis vnt.
01	Kenkimo PĮ	1 795	1 890	↓ 95
02	Informacijos rinkimas	1 005	1 187	↓ 182
03	Nepageidaujamų laiškų, klaidinančios informacijos platinimas	524	399	↑ 125
04	Mėginimas įsilaužti	210	278	↓ 68
05	DDoS atakos	98	43	↑ 55
06	Sėkmingas įsilaužimas	71	125	↓ 54
07	Neteisėta veikla, sukčiavimas	63	136	↓ 73
08	Kiti incidentai (atskiri, neatitinkantys nė vienos iš nurodytų grupių aprašymų)	314	30	↑ 284
Iš viso:		4 080	4 088	↓ 8

Vykdam socialinės inžinerijos atakas, kaip ir ankstesniais metais, aktyviai siųstos trumposios žinutės, skelbti pranešimai socialiniuose tinkluose ir el. laiškai su nuorodomis į interneto svetaines, imituojančias žinomas el. parduotuves, finansinių, siuntų ir kitų populiarių paslaugų teikėjų svetaines. Ypač pirmaisiais karo Ukrainoje mėnesiais buvo bandoma išnaudoti karo Ukrainoje tematiką ir imituoti žinomų pilietinių iniciatyvų ar kitų nevyriausybinių organizacijų, renkančių paramą ukrainiečiams, svetaines⁰².

^ 3 pav.

CERT-LT 2021–2022 m. dažniausiai fiksuotų kibernetinių incidentų statistika pagal grupes (šaltinis – NKSC)

Rekomendacijos, ką daryti nukentėjus nuo internetinių sukčių

Nedelsiant kreiptis į:

- ✓ savo banką, kurio prisijungimo duomenys ar ten laikomos lėšos galimai atiteko sukčiams;
- ✓ Lietuvos policiją, o apie imituojamus tinklalapius pranešti NKSC.

Panašios kibernetinių incidentų tendencijos fiksuojamos ir Europoje. Remiantis ENISA metine grėsmių apžvalga⁰³, antrojoje vietoje pagal dažnumą yra kenkimo PĮ, o trečiojoje vietoje – informacijos rinkimas naudojant socialinės inžinerijos įrankius. Pirmąją vietą ENISA skiria duomenis šifruojančiam kenksmingam programiniam kodui ir teigia, kad tai yra vienas iš dažniausiai Europoje pasitaikančių kibernetinių incidentų tipų. Šioms atakoms naudojamos nuolatos tobulėjančios puolimo technikos, atsiranda didesnė įrankių pasiūla tokiai veiklai vykdyti (angl. *Ransomware as a Service*, RaaS), tačiau esminė problema išlieka ta pati – pradiniai atakos vektoriai yra susiję su

03

ENISA Threat Landscape 2022, ENISA, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>.

socialine inžinerija, nesegmentuotais tinklais, žmogiškosiomis klaidomis administruojant sistemas (pavyzdžiui, paliekant numatytuosius (angl. *default*), pasikartojančius, nesudėtingus slaptažodžius ir pan.). DDoS atakos ENISA grėsmių sąrašė užima penktąją vietą, taip pat pažymima, kad jos tampa masiškesnės ir kompleksiškesnės, taikiniais pasirenkamos ne tik interneto svetainės, bet ir mobiliojo ryšio tinklai ir daiktų internetas (angl. *Internet of Things*, IoT).

2022 m. Lietuvoje, remiantis partnerių informacija ir automatinėmis priemonėmis apdorotais įvykiais, labiausiai paplitusi programinė įranga „Botnet“ tinkle, kurį sudaro daugiau kaip 13 tūkst. užvaldytų išmaniųjų įrenginių (**4 pav.**), buvo „Pykspa“. Išmanieji renginiai viešai pasiekiami per interneto ryšį arba turi bazinius ir nepakeistus slaptažodžius (pavyzdžiui, IP kameros, daiktų internetas ir pan.). Dažniausiai užvaldyti ir į „Botnet“ tinklą sujungti išmanieji įrenginiai yra naudojami DDoS atakoms vykdyti. Nuolat augant išmaniųjų įrenginių skaičiui ir tinkamai nesirūpinant jų saugumu, tikėtina, kad „Botnet“ tinklo naudojimo mastas ir galimybės tik didės.

4 pav. >
Lietuvoje 2022 m. fiksuotos „Botnet“ tinklo Pl (šaltinis – NKSC ir NKSC partneriai)

„Botnet“ tinklai	2022 m.
pykspa	13 091
qsnatch	6 978
nymaim	3 085
tinba	2 337
andromeda	2 310
matsnu	1 773
ranbyus	1 465
suppobox	734
zeus	722
pandabaker	371

Lietuvoje daugiausia kibernetinių incidentų 2022 m., kaip ir ankstesniais metais, fiksuota prieglobos paslaugų teikėjų infrastruktūrose (**5 pav.**), kurias galima naudoti interneto svetainėms, virtualioms darbo vietoms ar el. pašto paslaugoms kurti.

5 pav. >
Sektoriai, kuriuose CERT-LT 2022 m. fiksavo daugiausia kibernetinių incidentų (šaltinis – NKSC)

Sektorius	Incidentų skaičius
Prieglobos paslaugų teikėjai	1 620
Subjektai, valdantys ypatingos svarbos informacinę intrastruktūrą	850
Interneto paslaugų teikėjai	627

Tokį didelį incidentų skaičių nulėmė dvi priežastys: pažeidžiamos interneto svetainės ir galimybė Lietuvoje anonimiškai įsigyti prieglobos paslaugas. Dauguma prieglobos teikėjų suteikia galimybę už paslaugas atsiskaityti kriptovaliuta arba kitais nelegaliais būdais įsigytomis priemonėmis (pavyzdžiui, vogtais kreditinių kortelių duomenimis). Tai pirkėjams sukuria anonimiškumą, todėl gerokai apsunkina jų atsekamumą arba padaro jį iš viso neįmanomą. Internetiniai sukčiai, įsigiję prieglobos paslaugas, dažniausiai sukuria kenksmingas interneto svetaines arba svetaines, kuriose taikant socialinės inžinerijos metodus vagiama jautri informacija.

Pažeidžiamos interneto svetainės Lietuvos prieglobos teikėjų infrastruktūroje yra ilgametė ir opi problema. Interneto svetainės tampa pažeidžiamos, kai savininkas nesirūpina jos saugumu: laiku neatnaušina turinio valdymo sistemos, palieka kitas piktavalių lengvai išnaudojamas spragas, kuriomis pasinaudojus į tokią svetainę įkeliamas kenksmingas programinis kodas. CERT-LT aptikus ir vėliau savininkui nurodžius pašalinti kenksmingą programinį kodą, problema nėra išsprendžiama, nes paliktomis spragomis vėl pasinaudojama ir į svetainę įkeliamas kenksmingas programinis kodas. Taip oficiali svetainė tampa užpuolikų įrankiu, nuo kurio nukenčia tiek fiziniai, tiek juridiniai asmenys, užsienio subjektai.

Antroje vietoje pagal fiksuotų incidentų skaičių yra subjektai, valdantys ypatingos svarbos informacinių išteklius. Toks didelis incidentų skaičius yra siejamas su prievole kibernetinio saugumo subjektams apie visus kibernetinius incidentus pranešti NKSC, tačiau kiti juridiniai ar fiziniai asmenys tokios prievolės neturi ir apie patirtus incidentus NKSC praneša savanoriškai.

2 Karo Ukrainoje įtaka kibernetiniam saugumui

2022 m. vasario 24 d. prasidėjusi plataus masto invazija į Ukrainą turėjo didžiulę įtaką kibernetiniam saugumui visame pasaulyje.

Didesnės arba mažesnės kibernetinės atakos Ukrainoje buvo fiksuojamos nuolat, tačiau 2022 m. sausio mėn. jos suintensyvėjo. Sausio 13–14 d. atakuota daugiau kaip 70 Ukrainos vyriausybinių institucijų svetainių ir jose paskleista paniką kelianti dezinformacija rusų, ukrainiečių ir lenkų kalbomis. Išpuoliai tęsėsi ir vasario mėn., o likus kelioms dienoms iki karinės invazijos pradžios, surengtos dvi masinės kibernetinės atakos. Vasario 16 d. prieš šimtus Ukrainos interneto svetainių surengta DDoS ataka⁰⁴, o vėliau įvykdyta destruktvyi ataka prieš šimtus Ukrainos valstybinių informacinių sistemų, taip pat šalies energetikos, informacinių technologijų, žiniasklaidos ir finansų sektorius. Per ataką buvo naudojama duomenis naikinanti programinė įranga „HermeticWiper“⁰⁵ (angl. *wiper malware*). Pagrindinis šių atakų tikslas buvo pakirsti gyventojų pasitikėjimą Ukrainos valstybe ir vadovais, silpninti gyventojų valią priešintis.

Kare naudoti puolamieji kibernetiniai įrankiai peržengė valstybių sienas ir jų neigiamas poveikis buvo jaučiamas daug didesnėje teritorijoje. ES 2022 m. pirmą kartą istorijoje viešai apkaltino Rusiją, kad ji, likus kelioms valandoms iki masinio įsiveržimo į Ukrainą, įvykdė kibernetinę ataką prieš JAV palydovinio ryšio operatoriaus „Viasat“ valdomą palydovų tinklą KA-SAT⁰⁶, dėl kurios sutriko interneto tiekimas ne tik Ukrainoje, bet ir Vokietijoje, Prancūzijoje, Vengrijoje, Graikijoje, Italijoje ir Lenkijoje. Karas taip pat turėjo didžiulę įtaką kibernetinių aktyvistų (angl. *hacktivists*) grupuotėms, kurios stojo į priešingas kariaujančių šalių puses ir aktyviai jas rėmė. Ukrainą remiančios kibernetinių aktyvistų grupuotės, tokios kaip Ukrainos IT armija, skelbėsi įsilaužusios į Rusijos

04
Ukraine cyberattack is largest of its kind in country's history, says official | CNN, <https://edition.cnn.com/2022/02/16/europe/ukraine-cyber-attack-denial-service-intl/index.html>.

05
HermeticWiper: New data wiping malware hits Ukraine | WeLiveSecurity, <https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/>.

06
Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Consilium (europa.eu), <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>.

svarbiausias valdžios institucijas ir gavusios prieigą prie didžiulės apimties svarbios informacijos, sutrikdžiusios pagrindinių žiniasklaidos priemonių veiklą ir įvykdžiusios kitus žalingus veiksmus. Tuo metu prorusiška aktyvistų grupuotė „KillNet“ daugiausia skelbė apie didesnes ar mažesnes DDoS atakas tiek Europoje, tiek JAV.

Kibernetiniai išpuoliai prieš kritinę Ukrainos infrastruktūrą buvo vykdomi visus 2022 m. Karo pradžioje kibernetinės atakos buvo sudėtingesnės, joms rengtasi iš anksto, kartais net iki 6 mėn. Vėlesnių išpuolių atakos buvo paprastesnės, pavyzdžiui, DDoS atakos, socialinės inžinerijos principais paremti bandymai išvilioti jautrius duomenis, dezinformacijos platinimu ir pan.

Ukrainos kibernetinių incidentų valdymo komandos CERT-UA duomenimis, nuo masinės invazijos į Ukrainą pradžios 2022 m. vasario 24 d. iki 2023 m. vasario 1 d. CERT-UA iš viso užregistruoti 2 245 incidentai. Daugiausia fiksuota kenkimo programinės įrangos atvejų – 568, informacijos rinkimo – 552, sėkmingų įsilaužimų – 394 (**6 pav.**).

6 pav. >
CERT-UA registruotų kibernetinių incidentų statistika pagal kibernetinių incidentų grupes (2022 m. vasario 24 d.–2023 m. vasario 1 d.) (*Šaltinis – CERT UA*)

Kibernetinių incidentų grupės	Incidentų skaičius
Kenkimo PĮ	568
Informacijos rinkimas	552
Sėkmingas įsilaužimas	394
Kibernetinės spragos	222
Mėginimai įsilaužti	161
Kita	125

Daugiausia kibernetinių incidentų CERT-UA registravo valstybės ir savivaldybių srityje veikiančių organizacijų infrastruktūroje – 564, saugumo ir gynybos srityje – 312, verslo srityje – 159 (**7 pav.**).

7 pav. >
CERT-UA fiksuoti kibernetinių incidentų statistika pagal subjektų veiklos sritis (2022 m. vasario 24 d.–2023 m. vasario 1 d.) (*Šaltinis – CERT UA*)

Subjektai pagal veiklos sritis	Incidentų skaičius
Valstybės ir savivaldybių infrastruktūra	564
Saugumo ir gynybos infrastruktūra	312
Verslo įmonių infrastruktūra	159
Finansų infrastruktūra	120
Energetikos infrastruktūra	104
Telekomunikacijų ir programinės įrangos kūrėjų infrastruktūra	100
Transporto infrastruktūra	40
Kita	846

Reaguodamas į įvykius Ukrainoje ir pasikeitusią kibernetinio saugumo aplinką, NKSC aktyviai teikė rekomendacijas ir nurodymus kritinės infrastruktūros valdytojams dėl prevencinių kibernetinio saugumo priemonių taikymo, ypač daug dėmesio buvo skiriama veiklos tęstinumo planams. 2023 m. balandžio mėn. surengtos pratybos, išbandytas Saugusis valstybinis duomenų perdavimo tinklas ir įvertinti institucijų gebėjimai juo naudotis nutrūkus tarptautiniam interneto ryšiui⁰⁷.

Siekiant užtikrinti operatyvų informacijos apsikeitimą ir reagavimą į galimas grėsmes tarp kibernetinio saugumo subjektų ir NKSC, KSIT buvo sukurta uždara pokalbių platforma ir duomenų apsikeitimo modulis.

3 Kibernetinių incidentų prevencija ir kitos kibernetinį saugumą stiprinančios priemonės

2022 m. NKSC daug dėmesio skyrė valstybės ir ypatingos svarbos informacinių išteklių valdytojų darbuotojų atsparumui kibernetinėms grėsmėms. Kompleksinius trijų dienų kibernetinio saugumo mokymus baigė daugiau kaip 1 200 valstybės ir savivaldybių darbuotojų, 2 400 valstybės tarnautojų išklausė NKSC vykdytus trumpesnius mokymus įvairiomis bazinių kibernetinio saugumo žinių temomis. Specialus kursas buvo organizuotas paramą Ukrainai renkančioms Lietuvos organizacijoms. Perduotos žinios ir kompetencijos padeda darbuotojams tapti atsparesniems kibernetinėje erdvėje ir geriau pasirūpinti savo informacinių sistemų ir tinklų saugumu.

2022 m. spalio 18–20 d. NKSC, bendradarbiaudamas su KTU, surengė iki šiol didžiausias pagal dalyvių skaičių nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2022“. Jose dalyvavo 116 organizacijų, iš jų 107 – valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai.

Pratybose buvo naudojamas 2022 m. NKSC įdiegtas socialinės inžinerijos įrankis. Pasinaudojus šiuo įrankiu išsijusta daugiau kaip 56 tūkst. kibernetinių sukčių žinutes imituojančių el. laiškų. El. laiško neatpažino ir žalingus veiksmus atliko 7,1 tūkst. asmenų, arba beveik 13 proc. darbuotojų, tai rodo būtinybę vykdyti nuolatinį darbuotojų švietimą. Po pratybų dalyviams buvo surengti techniniai vienos dienos mokymai ir pademonstruota, kaip buvo galima ištirti pratyboms parengtus kibernetinius incidentus. Į mokymus užsiregistravo 237 dalyviai.

2022 m. NKSC įsigijo virtualų kibernetinio saugumo poligoną (angl. *Cyber Range*) ir pradėjo aktyviai organizuoti realaus laiko pratybas kibernetinio saugumo specialistams. Iš viso per metus poligono galimybėmis pasinaudojo ir savo profesines žinias sustiprino 163 Lietuvos ir 58 užsienio partnerių darbuotojai iš 47 organizacijų. Kibernetinio saugumo treniruoklis buvo panaudotas ir nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas 2022“. Šia galimybe pasinaudojo 92 dalyviai iš 25 organizacijų.

2022 m. NKSC koordinavo Lietuvos subjektų dalyvavimą didžiausiose ES kibernetinio saugumo pratybose „CyberEurope 2022“. Jose dalyvavo 8 didžiausios šalies asmens sveikatos priežiūros įstaigos, taip pat NKSC, Sveikatos apsaugos ministerija ir Registrų centras.

07
Išbandytas Saugiojo valstybinio duomenų perdavimo tinklas krizės atveju, <https://kam.lt/isbandytas-saugiojo-valstybinio-duomenu-perdavimo-tinklo-veikimas-krizes-atveju/>.

Kovai su žaibiškomis kibernetinėmis sukčiavimo atakomis, NKSC kartu su KTU Interneto paslaugų centru DOMREG sukūrė ir 2022 m. rudenį pristatė naują nemokamą įrankį gyventojams ir organizacijoms – DNS užkardą. Iki metų pabaigos ją buvo savanoriškai įsdiegę ne tik gyventojai ir verslo organizacijos, bet ir dalis ypatingos svarbos informacinių išteklių valdytojų.

NKSC 2022 m. kaip atskirą paslaugą pradėjo vykdyti kibernetinių grėsmių paiešką kibernetinio saugumo subjektų tinkluose. Per pirmuosius veiklos metus nustatytos 184 potencialios grėsmės, apie jas subjektai informuoti tiesiogiai arba per interneto paslaugų teikėjus. Taip pat buvo pradėtas vykdyti rankinis interneto svetainių spragų testavimas (angl. *manual vulnerability testing*). Per metus nustatytos 42 pažeidžiamos svetainės, dauguma jų viešojo sektoriaus. Keletas spragų nustatyta viešajame sektoriuje populiariose Lietuvos gamintojų diegiamose turinio valdymo sistemose, todėl realus pažeidžiamų svetainių skaičius galėjo būti didesnis, negu fiksuota NKSC.

Toliau vykdyta atsakingo atskleidimo koordinavimo veikla. 2022 m. NKSC sulaukė 51 pranešimo iš kibernetinio saugumo specialistų apie galimas spragas valstybinių institucijų interneto svetainėse. Buvo gauta vertingos informacijos apie svarbių sistemų saugumo spragas, tarp kurių viešajame sektoriuje populiari dokumentų valdymo sistema „Avily“ bei viešojo sektoriaus valdomos informacinės sistemos.

NKSC vykdė ypatingos svarbos informacinių išteklių patikrinimus, siekdamas nustatyti, kaip ypatingos svarbos informacinių išteklių valdytojai laikosi OTR. Per metus atlikti 6 patikrinimai (1 iš jų pakartotinis) energetikos, susisiekimo, civilinės saugos ir vandens tiekimo sektoriuose (2021 m. atlikti 5 patikrinimai). Jų metu nustatyti šie pagrindiniai ir pasikartojantys trūkumai: ypatingos svarbos informacinių išteklių valdytojai reguliariai neatlieka rizikos ir atitikties OTR, taip pat grėsmių ir pažeidžiamumų vertinimo, vykdoma nepakankama trečiųjų šalių priežiūra ir kontrolė (neužtikrinamas prieigos teisių valdymas, neatliekamas trečiųjų šalių atitikties vertinimas OTR, jų auditavimas). Vis dar daug funkcijų atliekama „ad hoc“ principu, nėra aiškiai apibrėžtų atsakomybių (paskirtų atsakingų asmenų) ir atskaitomybės už įgyvendinamus procesus.

Dėl vasarą įvykdytos masinės DDoS atakos ir duomenų šifravimo ir išpirkos reikalavimo atakų daugėjimo buvo atlikta ypatingos svarbos informacinių išteklių valdytojų apklausa. Siekta nustatyti ypatingos svarbos informacinių išteklių valdytojų taikomas priemones šioms atakoms atremti. Remiantis gautais rezultatais suformuluoti pasiūlymai tobulinti šiuo metu galiojančių OTR nuostatas, kurios įpareigotų ypatingos svarbos informacinių išteklių valdytojus taikyti papildomas saugos priemones. Per metus NKSC įvertino 279 valstybės informacinių išteklių saugos dokumentų, iš kurių 199 buvo pavirtinti, dėl kitų pateiktos pastabos. Siekiant patikrinti, kaip valstybės informacinių išteklių valdytojas laikosi saugos dokumentų reikalavimų, 2022 m. buvo atliktas vienas bandomasis tikrinimas ir suformuluoti siūlymai dėl teisėkūros pakeitimų, kad NKSC būtų suteiktos teisės nuolatos atlikti valstybės informacinių išteklių patikrinimus.

Atlikdamas Saugumo priežiūros tarnybos funkcijas, NKSC per metus gavo ir įvertino 152 įslaptintos informacijos ir ryšių informacinių sistemų saugos dokumentus, atliko 34 patikrinimus, išdavė 72 leidimus, suteikė daugiau kaip 200 įvairių konsultacijų.

2022 m. daug dėmesio skirta ir Krašto apsaugos sistemos duomenų perdavimo tinklo saugumui ir jo naudotojų švietimui. Kaip ir ankstesniais metais, krašto apsaugos sistemos naudotojams buvo surengtos iš anksto neskelbtos socialinės inžinerijos pratybos. Jų rezultatai, palyginti su 2021 m.,

rodo pažangą, nes 51 proc. sumažėjo vartotojų, atidariusių el. laišką pateiktą žalingą nuorodą, kartu padvigubėjo (114 proc.) atsakingų vartotojų, kurie pranešė apie kenkimo laišką Mil-CERT komandai.

NKSC toliau aktyviai vykdė tarptautinį bendradarbiavimą. 2022 m. gegužės mėn. NKSC pasirašė dvišalio bendradarbiavimo susitarimą (angl. *Memorandum Of Understanding*) su Lenkijos Nacionalinio kibernetinio saugumo centru – kibernetine vadaviete, o balandžio mėn. Lietuvos ir Lenkijos komanda užėmė antrąją vietą (iš 24) didžiausiose pasaulyje kibernetinės gynybos pratybose „Locked Shields 2022“.

2022 m. pavasarį NKSC specialistai kartu su JAV kariuomenės kibernetinės vadavietės atstovais sėkmingai įvykdė kibernetinės gynybos operaciją „Hunt Forward“. Pagrindinis operacijos tikslas buvo stiprinti praktinį sąveikumą ir didinti svarbiausių tinklų atsparumą kibernetinėms grėsmėms.

NKSC specialistai aktyviai dalyvavo ES Kibernetinio greitojo reagavimo veikloje. Vasario 21 d., reaguojant į įvykius Ukrainoje, ji buvo pirmą kartą aktyvuota. Vėliau dalyvavo pratybose Lietuvoje „Gintarinė migla 2022“ ir pratybose „CyberNet22“ Nyderlanduose, čia užėmė antrąją vietą. ES Kibernetinio greitojo reagavimo komandos atstovai 2022 m. taip pat dalyvavo mokymuose ir pratybose Rumunijoje.

2022 m. toliau buvo vykdoma RKGC plėtra. Per metus RKGC parengė ir su partneriais pasidalijo daugiau kaip 40 kibernetinių grėsmių žvalgybos ataskaitų bei kibernetinių įvykių analizių⁰⁸. 2022 m. rudenį buvo priimtas sprendimas dėl Lenkijos prisijungimo prie RKGC, o 2023 m. sausio mėn., pasirašius reikiamus susitarimus, Lenkija tapo RKGC nare. Taip pat buvo parengta Ukrainos kariuomenės kadetų praktikos mokymo programa ir baigtas bandomasis kursas. 2023 m. atliekama praktika RKGC Ukrainos kadetams leis įgyti žinių ir jas panaudoti tarnyboje, taip pat tai vienas iš Lietuvos paramos būdų kovojančiai Ukrainai.



Elektroninių ryšių tinklų vientisumo užtikrinimas ir draudžiamos viešai skleisti informacijos identifikavimas internete

Vadovo žodis



Jūratė Šovienė,
RRT tarybos pirmininkė

RRT nuolat skatina tvarią elektroninių ryšių infrastruktūros plėtrą bei ieško inovatyvių sprendimų draugiškesnei elektronei erdvei Lietuvoje ir pasaulyje. 2022 m. prasidėjęs Rusijos karas prieš Ukrainą išryškino elektroninių ryšių tinklų atsparumo bei internete pateikiamos informacijos svarbą valstybės saugumui.

Siekdami, kad elektroninių ryšių infrastruktūra būtų atspari, bendradarbiaudami su kitomis institucijomis bei rinkos dalyviais kelsime viešųjų elektroninių ryšių tinklų atsparumo ir stabilumo reikalavimus, taip didindami vartotojų galimybes gauti patikimas ir nepertraukiamas elektroninių ryšių paslaugas.

Kurdami švaresnę, saugesnę ir draugiškesnę skaitmeninę erdvę, stipriname bendradarbiavimą su Lietuvos policija ir informacijos prieglobos paslaugų teikėjais, naudojame dirbtinį intelektą grįstą įrankį „OxyCapture“ draudžiamo turinio Lietuvoje paieškai, taip pat aktyviai dalyvaujame tarptautinės interneto karštųjų linijų asociacijos INHOPE veikloje bei „Arachnid“ projekte.



KĄ SAUGO?

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



NUO KO SAUGO?

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



KAIP SAUGO?

- ✓ Dalyvaudama kaip tarpininkė informacijos apie vientisumo pažeidimus, kurie turėjo didelę įtaką viešųjų ryšių tinklų veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, sklaidai, ir užtikrindama, kad viešųjų ryšių tinklų teikėjai įgyvendintų tinkamas technines ir organizacines savo viešųjų ryšių tinklų vientisumo priemones.
- ✓ Vykdydama karštosios linijos „Švarus internetas“ veiklą ir kartu su partneriais imdamasi veiksmų, kad patyčios ir kita draudžiama skleisti informacija kuo greičiau būtų pašalinta, o neigiamą poveikį nepilnamečiams daranti informacija būtų atitinkamai pažymėta ir apribota.



1 RRT veikla, kuria prisidedama prie sklandaus interneto naudojimo

Šiuolaikinių valstybių gerovė nebeįsivaizduojama be elektroninių ryšių tinklų egzistavimo, sklandaus jų veikimo, todėl kyla vis didesnis poreikis užtikrinti nuolatinę kibernetinės erdvės pažangą ir tinklais teikiamų paslaugų įvairovę.

Elektroninių ryšių svarbą darniam valstybės funkcionavimui patvirtina ir tai, jog Lietuvos Respublikos Vyriausybės 2018 m. birželio 6 d. nutarime Nr. 556 „Dėl ūkinės veiklos sričių, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, sąrašo nustatymo“, be kita ko, nurodytos veiklos, susijusios su elektroninių ryšių paslaugų teikimu.

Nors RRT nevykdo funkcijų, užtikrinančių kibernetinį saugumą, tačiau dalimi veiklų prisideda prie to, kad asmenys galėtų sklandžiai naudotis internetu. Iš tokių RRT veiklų paminėtina viešųjų elektroninių ryšių tinklų teikėjų priežiūra, siekiant, jog būtų imtasi visų priemonių viešųjų elektroninių ryšių tinklų vientisumui užtikrinti, švaresnės interneto aplinkos kūrimas, patarimų interneto naudotojams teikimas, nepilnamečių apsauga nuo galimybės naršant internete susidurti su žalingu turiniu.

2 Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje

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

COVID-19 pandemija sukūrė elektroninių ryšių rinkos stabilumą – tiek inicijuotų skambučių trukmė, tiek perduodamų duomenų kiekis 2019 m. ir 2020 m. buvo gerokai išaugę (2020 m., palyginti su 2019 m., Lietuvoje pradėtų skambučių trukmė išaugo 17,2 proc., o perduodamų duomenų kiekis – 59,5 proc.), o neplanuotas paslaugų kiekio didėjimas kėlė riziką tinklų vientisumo užtikrinimui. Paslaugų teikėjai per dvejus pandemijos metus prisitaikė prie naujų poreikių, papildomai investavo į tinklus ir jų atsparumą, todėl 2021 m., kai situacija rinkoje stabilizavosi ir pradėtų skambučių trukmė pradėjo mažėti (per metus – 2,2 proc.), gerokai sumažėjo tikimybė atsirasti tinklų vientisumo pažeidimams, nors perduodamų duomenų kiekis vis dar augo (per metus – 28,3 proc.).

Atkreiptinas dėmesys, kad jau trečius metus iš eilės Lietuvoje mažėja pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus. 2022 m. RRT iš trijų teikėjų gavo 7 pranešimus – 3 pranešimai apie mobiliojo ryšio tinklo pažeidimus, 2 pranešimai apie mobiliojo ir fiksuotojo ryšio tinklų pažeidimus ir 2 pranešimai apie nacionalinės televizijos transliacijos sutrikimą ir nutrūkimą.

2020 m.			2021 m.			2022 m.	
Viešųjų ryšių tinklų vientisumo pažeidimų priežastys	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	
Elektros energijos tiekimo sutrikimai	1	1 000	–	–	2	32 946	
Kabelio nutraukimas, remontas	1	16 419	3	62 000	–	–	
Tarptinklinio ryšio paslaugų sutrikimai	–	–	–	–	–	–	
Tinklo įrangos gedimai	8	1 000 000 <	5	1 000 000 <	3	1 000 000 <*	
Kita	–		–	–	2	40 000	
Iš viso:	10		8		7		

1 pav. ^
Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys 2018–2022 m. (šaltinis – RRT)

* Viename iš pranešimų apie mobiliojo ryšio tinklo vientisumo pažeidimą nurodyta, kad pažeidimas paveikė galutinius paslaugų gavėjus visoje Lietuvoje.

2022 m. viename viešųjų ryšių tinklų vientisumo pažeidimo pranešime nurodyta, kad paveikti galutiniai paslaugų gavėjai visoje Lietuvoje. Šis pažeidimas truko 2 val. ir 8 min. ir buvo paveikti 38 proc. mobiliojo interneto naudotojų, kurie naudojo LTE technologiją, ir kalbinio ryšio naudotojai, kurie naudojo „VoLTE“ technologiją. Šis viešųjų ryšių tinklų vientisumo pažeidimas neišsiskyrė didesniu poveikiu galutiniams paslaugų gavėjams ir kaip kiti pažeidimai 2022 m. neatitiko Ekstremaliųjų įvykių kriterijų sąrašo, patvirtinto Lietuvos Respublikos Vyriausybės 2006 m. kovo 9 d. nutarimu Nr. 241 „Dėl Ekstremaliųjų įvykių kriterijų sąrašo patvirtinimo“⁰¹, 4.11–4.13 papunkčiuose nustatytų ekstremaliųjų įvykių trukmės kriterijų, dėl kurių apie pažeidimą reikėtų pranešti Lietuvos Respublikos Vyriausybės kanceliarijai, Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Vidaus reikalų ministerijos, Lietuvos Respublikos valstybės saugumo departamentui ir NKSC prie KAM.

01
Nuo 2023 m. sausio 1 d. Lietuvos Respublikos Vyriausybės 2022 m. gruodžio 29 d. nutarimu Nr. 1317 „Dėl Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo įgyvendinimo“ pripažintas netekusiu galios.

Lentelės eilutėje „Kita“ nurodomi viešųjų ryšių tinklų – mobiliojo ir fiksuotojo – pažeidimo atvejai. Šie du pranešimai susiję su interneto protokolo televizijos (IPTV) paslaugos sutrikimu. Apie šiuos paslaugų sutrikimus operatoriai gali pranešti RRT, nors jie ir neatitinka Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklėse⁰² nustatytų kriterijų.

Taigi, vertinant lentelėje pateiktus duomenis ir apibendrintą 2022 m. viešųjų ryšių tinklų vientisumo situaciją, pažymėtina, kad nepaisant vieno didesnio viešųjų ryšių tinklų vientisumo pažeidimo atvejo, viešųjų ryšių tinklų pajėgumai buvo ir yra pakankami, taip pat tinklai planuojami, stebimi ir vertinami atsakingai. Tokia išvada daroma iš teikėjų RRT pateiktų pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus, kas 3 mėnesius gaunamos papildomos informacijos iš teikėjų ir papildomai įvertinus RRT viešųjų elektroninių ryšių paslaugų kokybės matavimo rodiklius nuolatinės stebėsenos metu. Viešojo mobiliojo ir viešojo fiksuotojo ryšio tinkluose 2022 m. nebuvo fiksuojama daugiau gedimų nei ankstesniais metais, fiksuoti gedimai pašalinti operatyviai, o viešųjų ryšių tinklų vientisumo pažeidimų mastas nesukėlė ekstremalių įvykių, dėl kurių būtų reikėję imtis papildomų veiksmų ir (ar) informuoti kitas institucijas teisės aktų nustatyta tvarka.

3 Interneto karštosios linijos „Švarus internetas“ veikla ir interneto svetainės www.esaugumas.lt administravimas

Lietuvos Respublikos švietimo įstatymo 23² straipsnyje reglamentuojama pranešimų apie patyčias ir kitos pagal Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymą draudžiamos ar neigiamą poveikį nepilnamečiams darančios informacijos teikimo RRT tvarka, nustatyta RRT pareiga imtis veiksmų, kad draudžiama skleisti informacija būtų kuo greičiau pašalinta iš interneto, ir suteikta teisė duoti privalomus nurodymus (angl. *Notice and Take Down*, NTD) Lietuvos elektroninės informacijos prieglobos ar viešųjų ryšių tinklų paslaugų teikėjams dėl draudžiamos skleisti informacijos pašalinimo iš jų tarnybinių stočių arba prieigos prie jos panaikinimo, taip pat šių paslaugų teikėjų prievolė vykdyti privalomus RRT nurodymus.

RRT nuo 2007 m. yra įsteigusi ir administruoja interneto karštąją liniją, kurios pavadinimas nuo 2019 m. yra „Švarus internetas“ (www.svarusinternetas.lt). RRT administruojama interneto karštoji linija jau nuo 2008 m. yra tarptautinės interneto karštųjų linijų asociacijos INHOPE⁰³, vienijančios 50 interneto karštųjų linijų iš 46 šalių, narė. RRT, kaip ir kitų INHOPE asociacijos vienijamų interneto karštųjų linijų, pagrindinis tikslas – kad draudžiamas skleisti turinys būtų kuo greičiau pašalintas iš interneto. Ypač aktyviai INHOPE kovoja prieš vaikų seksualinio išnaudojimo vaizdus.

Karštąja linija „Švarus internetas“ visi interneto naudotojai gali pranešti apie internete pastebėtą draudžiamą skleisti ir neigiamą poveikį nepilnamečiams darančią informaciją, t. y. viešas patyčias kibernetinėje erdvėje naudojant vaizdinę informaciją; pornografinio turinio informaciją (įskaitant informaciją apie vaikų seksualinį išnaudojimą (pedofiliją); informaciją, kuria tyčiojamas, niekinama, skatinama neapykanta ar kurstoma diskriminuoti žmonių grupė ar jai priklausančių asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų, ir kitą įstatymais draudžiamą informaciją.

02
Ryšių reguliavimo tarnybos direktoriaus 2018 m. balandžio 25 d. įsakymas Nr. 1V-394 „Dėl Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių patvirtinimo“.

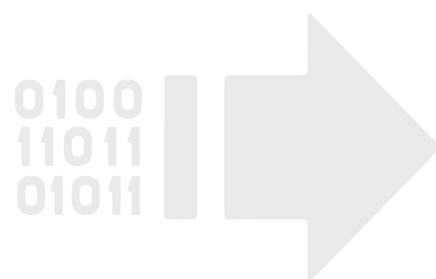
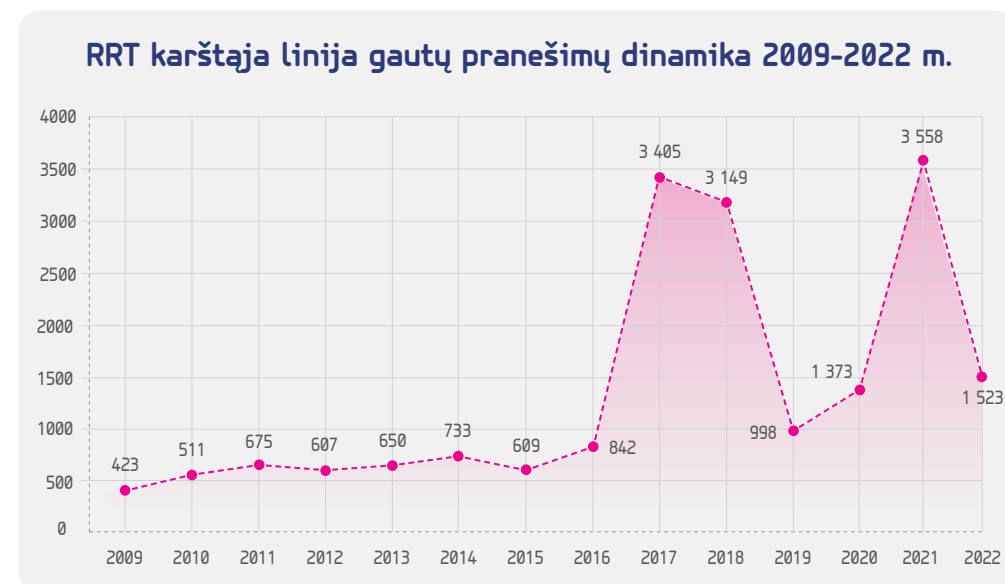
03
INHOPE, <https://www.inhope.org/EN>.

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

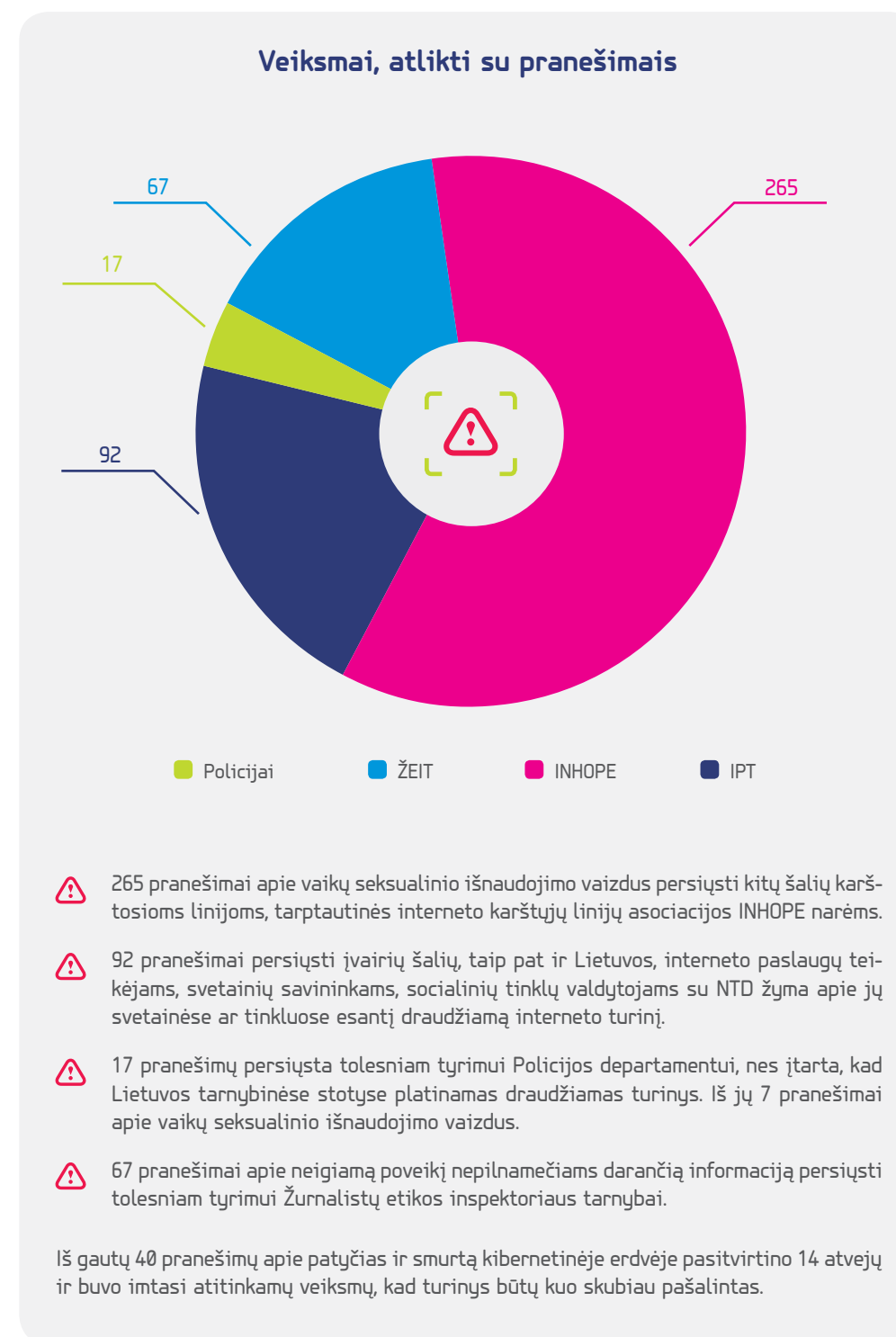
2022 m. RRT karštąja linija gauti 1 523 pranešimai apie internete pastebėtą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją (2 pav.).

2 pav. >

RRT karštąja linija gautų pranešimų dinamika 2009–2022 m. (šaltinis – RRT)



Pasitvirtino 694 pranešimai. Kadangi 253 pranešimai buvo pasikartojantys, tolesnių veiksmų imtasi dėl 441 atvejo (tai sudaro 29 proc. visų gautų pranešimų):



< 3 pav.

Veiksmai, atlikti su 2022 m. gautais pranešimais apie internete aptiktą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją (šaltinis – RRT)

Svarbu paminėti, kad RRT interneto karštąja linija gautų pranešimų skaičius nuolat kinta. 2022 m. gauta mažiau pranešimų apie vaikų seksualinio išnaudojimo vaizdus Lietuvos interneto erdvėje dėl to, kad 2021 m. buvo identifikuotas Lietuvos informacijos prieglobos paslaugų teikėjas, per kurio serverius buvo aktyviai viešinama vaikų seksualinio išnaudojimo medžiaga, ir informacija pašalinta. Į RRT karštąją liniją kreipiasi tiek atsakingi piliečiai, tiek tarptautinės interneto karštųjų linijų asociacijos INHOPE tinklo nariai ir pateikia itin tikslūs ir patikimus duomenis. Didėjantis žmonių sąmoningumas ir reagavimas į neigiamą turinį internete bei operatyvus bendradarbiavimas su policija duoda apčiuopiamų rezultatų.



Primename, kad interneto naudotojai apie neteisėtą (draudžiamą skelbti) ar žalingą (neigiamą poveikį nepilnamečiams darantį) turinį, aptiktą internete, skatinami pranešti karštosios linijos svetainėje www.svarusinternetas.lt/

RRT, savo iniciatyva vykdydama švietėjišką veiklą, taip pat administruoja interneto svetainę www.esaugumas.lt. Interneto svetainėje naudotojams teikiama informacija, kaip saugiai elgtis socialiniuose tinkluose, saugiai naudotis viešuoju belaidžiu internetu, elektronine bankininkyste, elektronine prekyba ar apsaugoti savo privatumą internete, kaip tinkamai pasirinkti antivirusinę programą ir t. t.

RRT specialistai teikia konsultacijas ir socialinių tinklų naudotojams. 2022 m. suteiktos 343 tokio pobūdžio konsultacijos, t. y. 21 proc. daugiau nei 2021 m. (284).

2022 m. interneto naudotojai dažniausiai susidūrė su šiomis problemomis:

- ⚠ socialinių tinklų paskyros užgrobimu;
- ⚠ paskyrų užblokavimu pažeidus socialinių tinklų taisykles;
- ⚠ neteisėtu asmeninės informacijos viešinimu;
- ⚠ prisijungimo prie paskyros duomenų praradimu.



Dirbtinio intelekto panaudojimas ieškant draudžiamo interneto turinio

Ankstesniais metais RRT kovos su draudžiamu ir neigiamą poveikį nepilnamečiams darančiu turiniu internete sėkmė priklausė nuo to, kad interneto naudotojai RRT karštąją liniją „**Švarus internetas**“ (www.svarusinternetas.lt) siuntė pranešimus, susijusius su pornografija, vaikų seksualinio išnaudojimu, smurtu ir pan. RRT, siekdama efektyvinti draudžiamos informacijos aptikimo procesą, nuo 2022 m. pradžios naudoja inovatyvų, dirbtiniu intelektu grįstą sprendimą – automatinį paieškos įrankį, kuriuo ieško draudžiamo turinio (pornografijos, vaikų seksualinio išnaudojimo medžiagos) Lietuvos interneto adresų (IP) erdvėje ir apie jį praneša RRT interneto karštajai linijai „**Švarus internetas**“.

Automatizuotas įrankis sukurtas „Oxylabs“ kompanijai bendradarbiaujant su RRT. Mokslo inovacijų ir technologijų agentūros „GovTech Lab“ iššūkių serijoje „Oxylabs“ sėkmingai įveikė RRT iškeltą iššūkį „Kaip automatizuotai identifikuoti draudžiamą interneto turinį?“ ir pateikė geriausią sprendimą. 2022 m. šiuo įrankiu patikrinta daugiau nei 288 tūkst. lietuviškų interneto svetainių – jose aptiktą galimai draudžiamą turinį vertino RRT tyrėjai, o faktui pasitvirtinus RRT ėmėsi konkrečių veiksmų. Nustatyta, kad 19 interneto svetainių galimai pažeidė nacionalinius Lietuvos ar ES įstatymus, o 8 pranešimai persiųsti tolesniam tyrimui Policijos departamentui, 11 pranešimų – Žurnalistų etikos inspektoriatui tarnybai.

Šis itin sėkmingas viešojo ir privataus sektoriaus bendradarbiavimo rezultatas pripažintas įvairiuose renginiuose: Baltijos šalių tvarumo apdovanojimuose įrankis nominuotas „Poveikio aplinkai“ kategorijoje ir užimta pirmoji vieta „Socialinių iniciatyvų“ subkategorijoje, Lietuvos dirbtinio intelekto asociacijos Metų apdovanojimuose įrankis nominuotas „Geriausio dirbtinio intelekto taikymo kategorijoje“, VŠĮ Inovacijų agentūros organizuojamuose „GovTech“ apdovanojimuose „Oxylabs“ ir RRT apdovanoti „Metų sėkmingiausio bendradarbiavimo“ kategorijoje. Siekdama kurti švaresnę, saugesnę ir draugiškesnę skaitmeninę erdvę, RRT planuoja įrankį tobulinti, kad būtų galima tiksliau aptikti draudžiamą turinį internete ir efektyviau atlikti RRT priskirtas funkcijas.



Kova su draudžiamu turiniu internete tarptautiniu lygiu. Dalyvavimas projekte „Arachnid“

RRT, ieškodama inovatyvių ir sėkmingai veikiančių įrankių, kurie padėtų kuo greičiau aptikti ir pašalinti draudžiamą interneto turinį, 2022 m. rugsėjo 29 d. pasirašė bendradarbiavimo sutartį su Kanados nevyriausybine organizacija „Canadian Centre for Child Protection“ dėl dalyvavimo jos vykdomame projekte „Arachnid“⁰⁴. Šiuo metu projekte – 13 interneto karštųjų linijų iš 12 šalių. Jau penkerius metus vykdomo projekto „Arachnid“ dalyviai ir partneriai sėkmingai kovoja su visame pasaulyje draudžiamu turiniu, susijusiu vaikų seksualinio išnaudojimu, aptikdami šį turinį ir siųsdami NTD pranešimus informacijos prieglobos paslaugų teikėjams visame pasaulyje, kad jie pašalintų draudžiamą turinį iš savo serverių. Išsiųsta daugiau kaip 20 mln. NTD nurodymų.

2022 m. pabaigoje RRT specialistai baigė keturių savaitių mokymus ir tapo visateisiais projekto „Arachnid“ dalyviais.

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

Švaresnės interneto aplinkos kūrimas, ypač nepilnamečiams, vienas svarbiausių RRT tikslų. RRT, siekdama šio tikslo, 2022 m. ragino prieigos prie viešųjų kompiuterių tinklų (internetu) paslaugas teikiančius asmenis (toliau – paslaugų teikėjai) įsidiesti privalomas, RRT aprobuotas filtravimo priemones (toliau – aprobuotos filtravimo priemonės) viešųjų kompiuterių tinklų (internetu) prieigos vietose, kur gali lankytis nepilnamečiai.

RRT, vadovaudamasi Lietuvos Respublikos Vyriausybės nustatyta prieigos prie viešųjų kompiuterių tinklų (internetu) vietose privalomų filtravimo priemonių naudojimo tvarka⁰⁵, aprobavo 10 filtravimo priemonių⁰⁶. 2022 m., kaip ir kasmet, RRT teikė paslaugų teikėjams konsultacijas ir metodinę medžiagą aprobuotų filtravimo priemonių pasirinkimo, diegimo, naudojimo klausimais, ragino paslaugų teikėjus naudojamas neaprobuotas filtravimo priemones teikti RRT aprobuoti.

2022 m. RRT atliko paslaugų teikėjų apklausą apie filtravimo priemonių naudojimą nepilnamečių ugdymo įstaigose, viešosiose bibliotekose. Apklausos rezultatai rodo vis didesnį paslaugų teikėjų supratimą ir poreikį apsaugoti nepilnamečius nuo žalingo interneto turinio, kai jie naršo mokyklų kompiuterinėse klasėse, bibliotekose ir viešųjų bibliotekų erdvėse. Aprobuotas filtravimo priemones naudojo 74 proc. apklausoje dalyvavusių paslaugų teikėjų, o per pastaruosius metus naudojimasis aprobuotomis filtravimo priemonėmis išaugo 18 procentinių punktų (2021 m. aprobuotas filtravimo priemones naudojo 56 proc. paslaugų teikėjų). Kasmet didėjantis aprobuotų filtravimo priemonių įstaigose poreikis rodo, kad RRT pastangos bendradarbiauti su ugdymo įstaigomis ir bibliotekomis, teikti konsultacijas telefonu ir el. paštu, skelbti interneto svetainėse www.rrt.lt ir www.esaugumas.lt interneto turinio filtravimo priemonių pasirinkimo, įdiegimo ir naudojimo rekomendacijas, duoda teigiamų rezultatų.

⁰⁴ Project Arachnid, <https://projectarachnid.org/en/>.

⁰⁵ Prieigos prie viešųjų kompiuterių tinklų (internetu) vietose privalomų filtravimo priemonių naudojimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2010 m. balandžio 28 d. nutarimu Nr. 463.

⁰⁶ Informacija apie aprobuotas filtravimo priemones, aprobuotų filtravimo priemonių sąrašas bei 2020–2022 m. apklausų rezultatų apžvalgą, <https://www.rrt.lt/saugesnis-internetas/turinio-filtravimo-priemones/>.

5 Karo Ukrainoje poveikis elektroninių ryšių tinklų saugumui

2022 m. vasario 24 d. prasidėjęs Rusijos karas prieš Ukrainą išryškino elektroninių ryšių bei internete pateikiamos informacijos svarbą valstybės saugumui. Nuo karo Ukrainoje pradžios išaugo pranešimų apie karo kurstymą, neapykantą skatinančią informaciją ir dezinformaciją skaičius, todėl aktyviai bendradarbiauta su Žurnalistų etikos inspektoriaus tarnyba (2022 m. išsiųsti 56, 2021 m. – 27 pranešimai).

Tarptautinė telekomunikacijų sąjunga pristatė 2022 m. atliktos ataskaitos apie karo padarytą žalą Ukrainos telekomunikacijų infrastruktūrai⁰⁷ rezultatus. Rengiant šią ataskaitą prisidėjo RRT ekspertas. Ataskaita apima aštuonis mėnesius nuo karo pradžios 2022 m. vasario 24 dieną. Rusijos karo Ukrainoje padaryti telekomunikacijų sektoriaus ekonominiai nuostoliai vertinami daugiau nei 0,1 mlrd., o norint atkurti Ukrainos telekomunikacijų sektoriaus 2022 m. sausį pasiektą lygį, reikia apie 1,79 mlrd. JAV dolerių. Ukrainos telekomunikacijų priemonėms, tinklams, sistemoms ir įrangai padaryta žala siekia 0,71 mlrd. JAV dolerių. Pasak RRT eksperto, tyrimas parodė, jog „IRT operatorių tinklai nuo karo pradžios buvo iš dalies, o kai kuriais atvejais ir visiškai sunaikinti arba užimti daugiau nei 10 iš 24 Ukrainos regionų. Per šešis karo mėnesius pranešta apie 1 123 kibernetines atakas, nukreiptas į visus Ukrainos ekonomikos sektorius, įskaitant IT ir telekomunikacijas“.⁰⁸

Vis dėlto Ukrainos telekomunikacijų sektorius yra atsparus, nepaisant karo sukeltų nuostolių, o remdamosi ataskaita Europos, kitos šalys bei tarptautinės organizacijos galės telkti finansinę ir techninę pagalbą, kad Ukrainoje būtų kuo skubiau atkurta kritiškai svarbi telekomunikacijų infrastruktūra ir ryšių paslaugos visoje Ukrainos teritorijoje. Paminėtina, kad karo veiksmai Ukrainoje vis dar tęsiasi, o agresorės (Rusijos Federacijos) veiksmai toliau didina žalą Ukrainos telekomunikacijų sektoriui, kitai svarbiai infrastruktūrai ir ekonomikai.

07

Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine, 2022, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.

08

RRT karštosios linijos pranešimų skaičių paveikė karas Ukrainoje, <https://www.rtt.lt/interneto-karstosios-linijos-skaicius-veike-karas-ukrainoje/>.



Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis



Renatas Požėla,
Policijos generalinis komisaras

Vadovo žodis

Kiekvienais metais susiduriame su vis didesnėmis kibernetinio saugumo grėsmėmis. Nemaža dalis nusikalstamų veikų jau seniai vyksta elektroninėje erdvėje, todėl policija labiau stebi ir kontroliuoja elektroninę erdvę.

Daug resursų skiriame pareigūnų pasirengimui tirti nusikaltimus elektroninėje erdvėje ir tam reikalingų kompetencijų lygiui kelti. Puikiai suvokiame, kad geresnės pareigūnų kompetencijos leidžia ne tik ištirti ir užkardyti nusikaltimus, bet ir taupo įstaigos bei valstybės resursus. Nusikaltėlių žinios kiekvienais metais vis gilėja, jie nuolat randa naujų būdų, kaip suklaidinti aukas, tad privalome kelti ir savo specialistų kvalifikaciją.

Žmogus elektroninėje erdvėje privalo jaustis toks pats saugus, kaip ir namuose ar gatvėje, tad kibernetiniam saugumui užtikrinti ir ateityje skirsime ypač daug dėmesio.



KĄ SAUGO?

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



NUO KO SAUGO?

- ✓ Nuo nusikalstamų veikų ir jų neigiamo poveikio.



KAIP SAUGO?

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



LIETUVOS POLICIJA
Ginti. Saugoti. Padėti.



www.epolicija.lt



info@policija.lt



112

1 Nusikalstamų veikų kibernetinėje erdvėje mastas, poveikis ir tarptautinės tendencijos

2021 m. Lietuvoje ir kitose Europos šalyse COVID-19 pandemija pakeitė daugelio žmonių įpročius. Karantino ribojimai, saviizoliacija pastūmėjo žmones į kibernetinę erdvę, o nusikaltėliai nusitaikė į jų finansinius išteklius. Besibaigiant pandemijai, visą Europą 2022 m. sukaustė dar viena sudėtinga geopolitinė situacija – karas Ukrainoje. Kol visuomenė telkėsi taikai, organizuoto nusikalstamumo veikėjai ieškojo naujų būdų pasipelninti.

Globaliame pasaulyje nusikaltėlių tinklai ir atskiri nusikalstamos veiklos dalyviai aktyviai veikia tarptautiniu mastu ir tarptautines krizes laiko veikiau galimybėmis nei apribojimais. Kaip pabrėžiama Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (toliau – Europol) 2022 m. gruodžio mėn. analitiniame leidinyje⁰¹, organizuotas nusikalstamumas pradedamas vykdyti per nuotolinio koordinavimo centrus (angl. *Remote coordination hubs for organised crime*). Valdydami nusikalstamas įmones ar struktūras nuotoliniu būdu, naudodamiesi nusikalstamų paslaugų ekonomika ir viso pasaulinio ryšio galimybių infrastruktūra, nusikalstamos veiklos dalyviai palaiko ryšius su tarpininkais ir partneriais, kontroliuojančiais kasdienes operacijas. Nuotolinis nusikalstamos veiklos koordinavimas yra rimtas išbandymas teisėsaugos institucijoms – išaiškinimo, keitimosi informacija ir baudžiamojo persekiojimo prasmėmis. Tačiau dėl glaudesnio tarptautinio bendradarbiavimo vis dažniau atsiranda galimybių kovoti su šiais nusikaltėliais. Europol bendradarbiavimas su trečiosiomis šalimis per darbo susitarimus turėtų suteikti daugiau galimybių ištirti ir išardyti visame pasaulyje koordinuotus tinklus, veikiančius nuotoliniu būdu.

Europolas identifikuoja tokias nusikalstamumo, siejamo su kibernetine erdve, vystymosi tendencijas:

1. Sukčiai dar labiau diversifikuoja metodus ir priemones, taip pat ir internete. Pavyzdžiui, sukčiai kuria suklustotas interneto svetaines, kurios atrodo beveik taip pat kaip tikros įmonių svetainės, prisistato kaip investavimo brokeriai, naudoja profesionalius skambučių centrus, klastoja investavimo dokumentus. Nusikalstami tinklai ir toliau plečia investicinių produktų portfelį.
2. Sandoriai, susiję su internetinio sukčiavimo schemomis ir bandymais sukčiauti, pradėjo atsirasti kibernetinėje erdvėje. Netikruose puslapiuose siūloma įsigyti skaitmeninių produktų. Siekiama užvaldyti ne tik įprastus finansinius, bet ir virtualius išteklius, turinčius finansinę išraišką.
3. „Emotet“ kenkimo PJ ir užvaldytų įrenginių tinklą (angl. *Botnet*), kurie laikomi vienais profesionaliausių ir atspariausių pasaulyje, naudojančios nusikaltėliai po pertraukos atnaujino savo veiklą. Nauja sukčiavimo banga el. laiškais įvairiomis kalbomis, kuriais „Emotet“ siekiama užkrėsti įrenginius, buvo aptikta visame pasaulyje. „Emotet“ naudojama kibernetinių nusikaltėlių, siekiančių gauti prieigą prie tinklo ar naudotojo paskyros ir diegti kitą kenkimo PJ, įskaitant išpirkos reikalaujančias programas.

⁰¹

Europol Analytical Brief, Recent Developments on Serious and Organised Crime and Terrorism, December 2022, Issue 08, REF: 2022-152.

4. Nusikaltėlių tinklai vagia automobilius keliose ES valstybėse, naudodami nelegaliai parduodamą konkrečių markių automobiliams skirtą diagnostikos priemonę, leidžiančią keisti transporto priemonėje esančią PJ.
5. Populiarėjant nepakeičiamiems žetonams, kibernetiniai nusikaltėliai kuria naujus būdus, kaip juos pavogti iš naudotojų. Vagystės dažnai vykdomos naudojant duomenų viliojimo (angl. *phishing*) kampanijas, kuriomis siekiama gauti prieigą prie jų kriptovaliutos piniginių. Kibernetiniai nusikaltėliai taip pat gali naudoti įsilaužimo ar domenų užvaldymo schemas, pagal kurias aukos įviliojamos į kenkimo interneto domenus, kurie nepastebimai skiriasi nuo teisėtų.
6. Atvirose šaltiniuose pateikta informacija ir socialinės žiniasklaidos platformose stebėtos transliacijos atskleidė daugybę atvejų, kai perkeltieji asmenys, įskaitant vaikus, pasirodė gyvai transliuojamose socialinės žiniasklaidos platformose, prašydami aukų ar paaukoti skaitmeninių dovanų, turinčių piniginę vertę. Nors jokios oficialios informacijos, ar tokie elgetavimo internete faktai gali būti susiję su organizuotu nusikalstamumu, šiuo metu nėra, neatmetama rizika, kad jie gali būti susiję su išnaudojimu prievartiniam elgetavimui internete. Toks priverstinis elgetavimas gali būti susijęs su sukčiavimo internete schemų organizavimu, apgaudinėjant socialinės žiniasklaidos naudotojus, įskaitant ES gyventojus.

2 Nusikaltimų kibernetinėje erdvėje Lietuvoje tendencijos

Vertinant Lietuvos visuomenės socialinio gyvenimo aktualijas, komunikavimo bei vartojimo įpročius, spar-tėjančią paslaugų, teikiamų per elektroninę erdvę, plėtrą, taip pat investicijas į skaitmenizacijos procesus, tikėtina, kad nusikaltimai kibernetinėje erdvėje 2023 m. progresuos, o pagrindinis motyvas liks pasipelnymas.

Vis aiškiau matoma tendencija, kad nusikalstamas veikas Lietuvoje vykdančias asmenys veikia ne pavieniui, o gerai organizuotose grupėse, kurias identifikuoti, kaip ir tokio pobūdžio nusikalstamas veikas ištirti, yra sudėtinga ir komplikuota dėl technologijų gausos, teisinių sunkumų, susijusių tiek su tokių veikų padarymo vietos nustatymu, tiek ir su ikiteisminiam tyrimui reikšmingų duomenų (informacijos) gavimu iš trečiųjų šalių. Nuo šių nusikalstamų veikų nukenčia ne tik Lietuvos, bet ir užsienio fiziniai ir juridiniai asmenys.

Internetinės nusikaltėlių bendruomenės yra itin pažengusios ir nuolat tobulėja. Sukčiai vis dažniau naudoja pažangiomis technologijomis savo anonimiškumui apsaugoti. Jie naudoja internetinėmis duomenų saugyklomis ir taiko pažangius šifravimo metodus, kad apsaugotų nuo policijos vykdomos stebėsenos ir skaitmeninės ekspertizės. Tyrimus taip pat apsunkina tai, kad dalis nusikalstamų veikų organizuojamos ir vykdomos iš trečiųjų šalių.

3 Kibernetiniai nusikaltimai plačiąja prasme

Nusikaltimai elektroninėje erdvėje plačiąja prasme apibrėžiami kaip bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo panaudotos kompiuterinės technologijos, o nusikaltimo faktui įrodyti turi būti taikomos specifinės nusikaltimų elektroninėje erdvėje tyrimo priemonės.

2022 m. dominavęs kibernetinių nusikaltimų (tiek plačiąja, tiek siaurąja prasme) motyvas buvo nusikalstamas pelnymas (83 proc.). Kiti dažni, tačiau aukštais rodikliais nepasižymėję motyvai (tikslai) buvo kibernetinis chuliganizmas (5 proc.) ir duomenų apie informacinių sistemų pažeidžiamumą ieškojimas ir (ar) elektroninių duomenų grobimas (3 proc.).

2022 m. šalies policijos įstaigose užregistruotos 42 988 nusikalstamos veikos, iš kurių 5 309 nusikalstamos veikos, arba 12 proc., padarytos kibernetinėje erdvėje. 2022 m. nusikalstamų veikų kibernetinėje erdvėje, palyginti su 2021 m., padaugėjo 2 775 atvejais, arba 52 proc. Bendroje nusikalstamumo struktūroje 2022 m. nusikalstamų veikų, padarytų kibernetinėje erdvėje, dalis padidėjo 6 proc., palyginti su 2021 m. 2022 m. nusikalstamų veikų, padarytų fizinėje aplinkoje, palyginti su 2021 m., padaugėjo 495 nusikalstamomis veikomis, arba 1 proc. Tai rodo, kad 2022 m. registruoto nusikalstamumo augimą labiausiai lėmė nusikalstamos veikos elektroninėje erdvėje.

Kaip ir pastaruosius kelerius metus, 2022 m. nusikalstamumą elektroninėje erdvėje labiausiai lėmė sukčiavimo (LR BK 182 str.) atvejai, jie 2022 m. sudarė didžiąją – 48 proc. – dalį visų kibernetinėje erdvėje padarytų nusikalstamų veikų. Nusikalstamumui elektroninėje erdvėje didelę įtaką taip pat turi šios penkios nusikalstamos veikos:

- ⚠ neteisėtas prisijungimas prie informacinės sistemos (LR BK 198¹ str.) – **16 proc.**;
- ⚠ neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (LR BK 215 str.) – **15 proc.**;
- ⚠ netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis (LR BK 214 str.) – **9 proc.**;
- ⚠ disponavimas pornografinio turinio dalykais (LR BK 309 str.) – **5 proc.**;
- ⚠ kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (LR BK 170 str.) – **2 proc.**

Sukčiavimo būdu padaryta žala

Lietuvos kriminalinės policijos biuro duomenimis, išviliotų pinigų suma sukčiavimo atveju svyravo nuo kelių dešimčių eurų iki lėšų, siekiančių milijonines sumas. 2022 m. dažniausiai (58 proc. atvejų, arba 27 proc. daugiau nei 2021 m.) išviliotų pinigų sumos buvo iki 1 000 eurų. Didžiausių žalų, kai lėšos viršijo 10 000 eurų, atvejai 2022 m. sudarė 8 proc. (arba 24 proc. daugiau nei 2021 m.).

Lietuvos policijos informaciją apie elektroninį sukčiavimą papildė ir LBA surinkti duomenys apie finansinį sukčiavimą ir jo padarytą žalą⁰². LBA duomenimis, finansiniai sukčiai iš Lietuvos gyventojų ir įmonių 2022 m. išviliojo beveik 12 mln. eurų⁰³.

02

Atkreipiame dėmesį, kad LBA užfiksuotų elektroninių sukčiavimų atvejų ir policijos įstaigose pradėtų ikiteisminių tyrimų dėl sukčiavimo kibernetinėje erdvėje skaičius yra ne toks pats.

03

LBA duomenys, <https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/finansiniai-sukciai-pernai-iviliojo-12-mln-euru-savininkams-grazinti-5-mln-euru>.

Tuo pačiu laikotarpiu finansų įstaigų bei teisėsaugos pastangomis savininkams buvo grąžinta apie 5 mln. eurų. Nors apgaule išviliotų lėšų suma didėjo palyginti nedaug (2021 m. išviliota 10,2 mln. eurų), užfiksuotų incidentų skaičius paaugo daugiau nei dvigubai. 2021 m. gyventojų ir verslo nuostolių, patirtų dėl finansinių sukčių schemų, metinis augimas buvo dvigubas – prarastų lėšų suma sudarė daugiau kaip 10 mln. eurų, kai tuo metu 2020 m. – apie 5 mln. eurų. Savo ruožtu per praėjusius metus, palyginti su 2021 m., nuo 3,5 tūkst. iki bemaž 8 tūkst. išaugo incidentų skaičius. Šie statistikos rodikliai rodo ne tik augantį sukčių aktyvumą, bet ir didesnį visuomenės atvirumą šia tema – nukentėjusieji drąsiau pasakoja apie savo patirtį, aktyviau praneša bankams apie patirtą arba gresiantį sukčiavimą.

Kilus įtarimų, kad gyventojai arba verslo atstovai jau užkibo ant sukčių kabliuko, klientų patvirtintas operacijas bankai sustabdo, o kartais pavyksta susigrąžinti ir į kitas finansų įstaigas jau pervestas lėšas. Finansų sektoriaus specialistai primygtinai ragina nepažįstamiesiems, kad ir kuo jie prisistatytų esantys ir kokias istorijas pasakotų, neatskleisti savo prisijungimo prie elektroninės bankininkystės duomenų, neatidarinėti el. pašto ar SMS žinutėmis nelauktai atsiųstų nuorodų, neskubėti reaguoti į gąsdinančias žinutes ar skambučius, kuriais pranešama apie neva užblokuotas paskyras, sąskaitas ir pan.

LBA žiniomis, gyventojų sąmoningumą bei gebėjimą kritiškai mąstyti skatina aktyvi komunikacija. Praėjusiais metais LBA ir 20 jos vienijamų finansų įmonių kartu su Lietuvos policija, Lietuvos banku bei kitais partneriais, be individualių iniciatyvų ir operatyvaus informavimo apie vykstančias sukčių atakas, vykdė informacinę kampaniją „Atpažink sukčių“. Projekto interneto svetainėje www.atpazinksukciu.lt ir pasibaigus aktyviam kampanijos etapui apžvelgiamos dažniausios nusikaltėlių kaukės arba scenarijai.

Sukčiavimo tendencijos

Dominuojantys sukčiavimo būdai:

⚠️ Avansinio (išankstinio mokėjimo) sukčiavimo tendencija (32 proc.):

2022 m. avansinio (išankstinio mokėjimo) sukčiavimo atvejų, palyginti su 2021 m., padaugėjo 12 proc. Pagrindinis avansinio (išankstinio mokėjimo) sukčiavimo būdas yra apgaulingų skelbimų platinimas internete ir išprovokavimas virtualiai susitarti ir atlikti mokėjimą į sukčiaus nurodytą sąskaitą (90 proc.). 2022 m. iš apgaulingų skelbimų dominavo pasiūlymai pirkti mobiliuosius telefonus ir (ar) kompiuterių techniką, transporto priemones, išsinuomoti nekilnojamąjį turtą, pirkti nekilnojamąjį turtą, pirkti kuro briketus. Apgaulingi skelbimai buvo platinami nacionaliniuose reklamos portaluose, dažniausiai *skelbiu.lt*, *autoplius.lt* ir *alio.lt*. Kita dažnai naudota apgaulingų skelbimų platinimo erdvė buvo socialinio tinklo „Facebook“ grupės. Nors apgaulingų skelbimų platinimas tarptautinėse reklamos platformose nėra dažnas reiškinys, 2022 m. tirti atvejai rodo, kad apgaulingi skelbimai dažniausiai buvo platinami Vokietijos reklamos svetainėje *mobile.de*. Svarbiausios apgaulingo avansinio (išankstinio) mokėjimo komunikavimo priemonės 2022 m. nekito – dominavo naudojimas nacionaliniu telefoniniu ryšiu. Kitas dažnas komunikavimo būdas buvo naudojimas elektroninio bendravimo programėlėmis, dažniausiai „Facebook“ programėle „Messenger“.



2022 m. atskleisti sisteminiai avansinio sukčiavimo atvejai, kuriuos organizavo Marijampolės kalėjime laisvės atėmimo bausmės atliekančių nuteistųjų grupė, pasižymėjo išradingai pritaikyta nusikalstamu būdu gautų lėšų legalizavimo schema. Sukčiai nusikalstamu būdu gautoms lėšoms legalizuoti pasinaudojo įmonių, prekiaujančių gėlėmis, netyčinėmis paslaugomis. Avansinio sukčiavimo organizatoriai internetu užsakydavo puokštės pristatymo paslaugą, taip pat susitardavo dėl lėšų, pervestų į parduotuvių sąskaitas, išgryninimo. Parduotuvės, vykdydamos kliento užsakymą, įteikdavo per dovanų kurjerį nurodytam adresatui puokštę ir grynuosius pinigus voke.

Kiti 6 dažniausi sukčiavimo būdai bendrai sudaro 49 proc. ir apima tokias nusikalstamas veikas kaip:

⚠️ Telefoninis sukčiavimas (17 proc.):

2022 m. naudojimas apgaulingomis SMS žinutėmis iš visų telefoninio sukčiavimo atvejų sudarė 51 proc.

Pagrindinis sukčiavimo, kai siunčiamos apgaulingos telefoninės SMS žinutės, tikslas yra grobstymas iš svetimų sąskaitų. SMS žinutėse teikiamos nuorodos į suklustotas svetaines ir išprovokuojama įvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos. Visos apgaulingos telefoninės SMS žinutės buvo platinamos dangstantis finansų įstaigų ir (ar) jų informacinių sistemų vardu.

2022 m. apgaulingi telefoniniai skambučiai iš visų telefoninio sukčiavimo atvejų sudarė 49 proc. Apgaulingus telefoninius skambučius labiausiai lėmė grobstymo iš svetimų sąskaitų motyvas (65 proc.). 2022 m. dominavo apgaulingi apsimetėlių bankų darbuotojų ir teisėsaugos pareigūnų telefoniniai skambučiai, kuriais buvo pranešama apie elektroninės bankininkystės problemas ir nukentėjusieji provokuojami perduoti elektroninės bankininkystės duomenis arba prisijungti prie elektroninės bankininkystės paskyrų ir patvirtinti apgaulingai inicijuotus lėšų iš sąskaitos pavedimus.

2022 m. atvejai, kai apgaulingais telefoniniais skambučiais buvo išprovokuojama perduoti grynuosius pinigus ir (ar) vertybes, sudarė 34 proc. Tokiais atvejais dažniausiai apsimetę nusikaltėliai policijos pareigūnais pranešdavo apie namuose laikomus netikrus pinigus ar apsimetę artimaisiais pranešdavo apie atsitikusią nelaimę ir išprovokuoti nukentėjusieji perduodavo grynuosius pinigus (ir) ar vertybes į namus atsiųstiems telefoninių sukčių bendrininkams.



2022 m. atsirado nauja telefoninių sukčių kategorija – tariamieji interneto platformų administratoriai (bendraujantys anglų, rusų kalbomis). Tiriama atvejai rodo, kad pirma skambina apsimetėliai „Google“ platformos darbuotojai ir informuoja apie tariamas „Gmail“ pašto paskyrų problemas ir būtinumą suteikti diagnostikos paslaugas, išprovokuoja įsidięti nuotolinės prieigos programas, įgyja prisijungimo prie įrenginių ir (ar) paskyrų, įskaitant ir elektroninės bankininkystės paskyras, duomenis, tariamai nustato sąskaitų saugumo riziką ir apie tai tariamai informuoja bankus. Vėliau skambina apsimetėliai bankų darbuotojai ir išprovokuoja nukentėjusiuosius atskleisti kitą dalį elektroninės bankininkystės duomenų ir (ar) patvirtinti apgaulingai inicijuotus pavedimus iš sąskaitų.

⚠️ Apgaulingos internetinio bendravimo programų žinutės (8 proc.):

2022 m. atvejai, kai buvo naudojamos apgaulingomis internetinio bendravimo programų žinutėmis, išsiskyrė ypač sparčiai didėjančiu skaičiumi, palyginti su 2021 m. (68 proc. daugiau). Pagrindinis sukčiavimo, kai siunčiamos apgaulingos žinutės, tikslas yra grobstymas iš svetimų sąskaitų. Žinutės su nuorodomis į suklustotas svetaines siunčiamos vartotojui ir išprovokuojama įvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos.

2022 m. didžiąją dalį apgaulingų internetinio bendravimo programų žinučių gavo daiktus internete parduodantys asmenys iš apsimetėlių pirkėjų (81 proc.). Kitą didesnę dalį sudaro apgaulingos internetinio bendravimo programų žinutės, kurias gavo elektroninės bankininkystės vartotojai

tariamai iš elektroninės bankininkystės informacinių sistemų (13 proc.). 2022 m. apgaulingomis internetinio bendravimo programų žinutėmis dažniausiai buvo platinamos nuorodos į šias suklas-totas interneto svetaines: DPD, „Omniva“, „Vinted“, „LP Express“. 2022 m. naujas reiškinys buvo svetainių „Vinted“ ir „Omniva“ klastojimas, taip pat didėjo naudojimosi suklas-totomis DPD ir „LP Express“ svetainėmis rodikliai. Nuo 2020 m. matoma ilgalaikė sukčiavimo dinamikos tendencija rodo, kad naudojimosi suklas-totomis DPD, „Omniva“, „Vinted“, „LP Express“ svetainėmis lygis kasmet nuosekliai didėja ir pasižymi ypač rizikinga dinamika.



2022 m. išryškėjo nauja tendencija – sukčiavimas taikant apgaulingų in-ternetinio bendravimo programų žinučių schemą. Pagrindine priemone yra tapusi programėlė „WhatsApp“, o naudojimosi programėle „Viber“ atvejų skaičius yra stipriai sumažėjęs.

⚠️ Prekės ar paslaugos įgijimas sukčiavimo būdu (7 proc.):

2022 m. atvejų, kai sukčiavimo būdu buvo įgytos prekės ar paslaugos, gerokai sumažėjo, palyginti su 2021 m. (54 proc. mažiau). Pagrindinis prekių ar paslaugų įgijimo sukčiaujant būdas yra internete daiktus parduodančių asmenų apgaudinėjimas (66 proc.). Tokie atvejai dažniausiai susiję su pardavėjo išprovokavimu išsiųsti prekę, kai jam pateikiamas pranešimas apie atliktą mokėjimą, nors iš tikrųjų tai yra suklas-toto pavidimo kopija. 2022 m. sukčiavimo būdu dažniausiai buvo įgyjama elektroninė technika, laisvalaikio ir pramogų priemonės, buitinė technika, darbo priemonės, transporto priemonių dalys.

⚠️ Apgaulingi el. laiškai (angl. phishing) (7 proc.):

2022 m. apgaulingų el. pašto laiškų gerokai padaugėjo, palyginti su 2021 m. (71 proc. daugiau). Pagrindiniai apgaulingų laiškų tikslai: elektroninės bankininkystės vartotojų išprovokavimas (75 proc.), įsiterpimas į sandorio šalių susirašinėjimą (17 proc.), įsiterpimas į organizacijų personalo susirašinėjimą (8 proc.). 2022 m. didžiausią 457 142 eurų žalą patyrė Vilniaus draudimo bendrovė, kai buvo įsiterpta į elektroninį susirašinėjimą ir apgaulingai nurodyta banko sąskaita.

2022 m. atsirado ir išplito naujas reiškinys – elektroninės bankininkystės vartotojų išprovokavimas atsidaryti apgaulingais el. pašto laiškais gautas nuorodas į suklas-totas svetaines ir suvesti elek-troninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavidimą iš sąskaitos. Apgaulingi el. laiškai dažniausiai buvo platinami daiktų pardavimo interneto platformos „Vinted“ pardavėjams (44 proc.). 15 proc. sudarė atvejai, kai dangstantis siuntų tarnybų vardu reikalauta apmokėti siuntos mokestį, nukentėjusieji gavo apgaulingus el. laiškus su nuorodomis į suklas-totas svetaines ir buvo išprovokuoti suvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavidimą iš sąskaitos. 14 proc. sudarė atvejai, kai dangstantis bankų ar jų platformų informacinių sistemų vardu siųsti pranešimai apie elektroninės bankininkystės problemas, elektroninės bankininkystės vartotojai gavo apgaulingus el. laiškus su nuorodomis į suklas-totas svetaines ir buvo išprovokuoti suvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavidimą iš sąskaitos.

LBA taip pat išskiria duomenų viliojimą (angl. *phishing*) kaip bene labiausiai paplitusį sukčiavimo būdą. 2022 m. LBA nariai užfiksavo 3 500 duomenų viliojimo atvejų, t. y. beveik tris kartus daugiau nei 2021 m., nuostoliai išaugo nuo 800 tūkst. iki 2 mln. eurų. Taip pat daugiau kaip šimtu atvejų padaugėjo registruoto romantinio sukčiavimo – nuo 195 iki 322, tačiau dėl šio scenarijaus patirtų nuostolių suma per metus pakito nedaug (2021 m. – 641 tūkst. eurų, 2022 m. – 650 tūkst. eurų).

LBA duomenys papildė Lietuvos policijos pateiktą informaciją apie susirašinėjimo el. paštu perė-mimą. Teigiama, kad siunčiant suklas-totus apmokėjimo dokumentus dažniausiai buvo taikomasi

į verslo organizacijas bei įstaigas. Šis būdas lieka daugiausia individualių nuostolių padarančiu sukčiavimo būdu – nukentėjusios įmonės 2022 m. neteko vidutiniškai apie 28 tūkst. eurų per vieną nusikaltimą. Per praėjusius metus šio scenarijaus padaryti nuostoliai sudaro 2,6 mln. eurų, bemaž tiek pat, kiek 2021 m.

2022 m. įvykių, kai buvo įsiterpta į sandorio šalių elektroninį susirašinėjimą, palyginti su 2021 m., sumažėjo (23 proc. mažiau). Pagrindinis tokio sukčiavimo tikslas buvo perimti sandorio šalių elektroninį susirašinėjimą ir mokėjimo šaliai pateikti apgaulingą el. pašto laišką su reikalavimu pavidimą atlikti į pakeistą banko sąskaitą. 2022 m. įvykių, kai buvo įsiterpta į personalo susira-šinėjimą, ne itin padaugėjo (33 proc. daugiau nei 2021 m.). Pagrindinis tokio sukčiavimo tikslas buvo adresuoti įstaigų ar įmonių finansininkams apgaulingus el. laiškus su tariamai vadovaujančio personalo tarnybiniais nurodymais atlikti mokėjimą į sukčiaus sąskaitą.

⚠️ Investicinis sukčiavimas (6 proc.):

Lietuvos policijos duomenimis, 2022 m. investicinio sukčiavimo atvejų, palyginti su 2021 m., ge-rokai padaugėjo (35 proc. daugiau). 2022 m. didžioji dalis (77 proc.) investicinio sukčiavimo atvejų buvo apgaulingų investavimo platformų reklamos platinimas internete, išprovokavimas reklamos anketose užregistruoti kontaktinius duomenis ir telefoninio ir (ar) internetinio komunikavimo būdu skatinimas atlikti pavidimus į tariamai investavimui skirtas sąskaitas, kurias sukčiai kontroliuoja, iš jų persiveda ir pasisavina lėšas. Apgaulingų investavimo platformų reklamos anketos yra pritaikytos potencialių nukentėjusiųjų tapatybės ir kontaktiniams duomenis rinkti, profesionaliai jiems tvarkyti duomenų bazėse, kurios užtikrina galimybę manipuluoti nukentėjusiųjų pasitikėjimu ir kartojamais ciklais viliooti iš jų pinigus.

Kita dažniausia investicinio sukčiavimo schema yra telefoninių sukčių atakos, kai anksčiau nuo investicinio sukčiavimo nukentėjusiems asmenims pasiūloma tarama pagalba susigrąžinti prarastas lėšas (17 proc.). Neretai naudojama schema, kai telefoniniai sukčiai, bauginami, kad nusikals-tamos struktūros perėmė ir neteisėtiems tikslams naudoja investicines sąskaitas, išprovokuoja dėl investicinio sukčiavimo anksčiau nukentėjusius asmenis (iki 1 proc.). Pasakojimai atskleidžia ypač gerai organizuotą investicinio sukčiavimo subjektų veiklą. 2022 m. atsirado naujas reiškinys – apgaulingos lažybos, kai internete platinant reklamą išprovokuojama atlikti statymus (6 proc.).

LBA duomenimis, 2022 m. investicinio sukčiavimo, kai žmonėms žadama garantuotai didelė grąža už įdėtus pinigus, užfiksuotų incidentų skaičius augo nuo 576 atvejų 2021 m. iki 852 atvejų 2022 m., tačiau per metus pagal šią schemą išviliotų lėšų suma mažėjo nuo 3 mln. iki 2 mln. eurų.

⚠️ Grobstymas iš sąskaitų, kai nebuvo taikoma socialinė inžinerija (4 proc.):

2022 m. grobstymo iš sąskaitų be socialinės inžinerijos požymio atvejų gerokai išaugo (44 proc. daugiau nei 2021 m.). 2022 m. didžioji dalis grobstymo iš sąskaitų atvejų buvo neteisėtas pasi-naudojimas mokėjimo kortelėmis (53 proc.), 26 proc. – grobstymas iš sąskaitų susijusių asmenų aplinkoje, 21 proc. – neteisėtas elektroninės bankininkystės vartotojų duomenų panaudojimas.

⚠️ Nuotolinės prieigos programos:

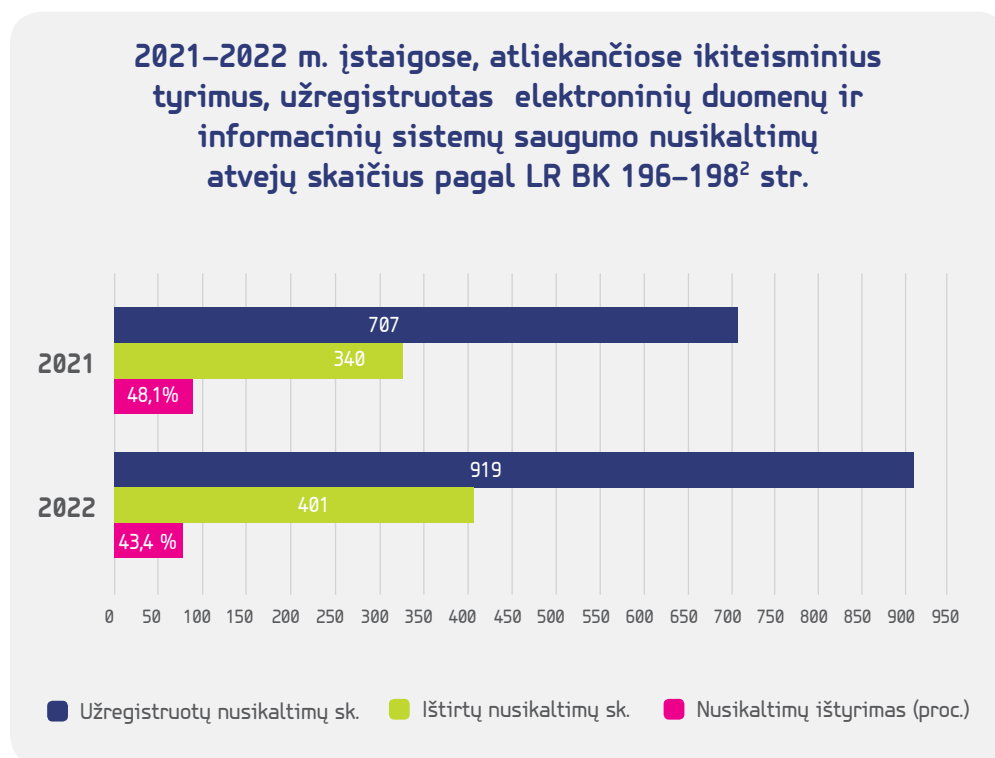
2022 m. kibernetinių nusikaltimų schemose ir toliau dažniausiai naudotasi nuotolinės prieigos programine įranga „AnyDesk“. Nuotolinės prieigos programinė įranga taip pat dažniausiai nau-do-jama investicinio ir telefoninio sukčiavimo schemose, kai išprovokuoti nukentėjusieji įsidiegė nuotolinės prieigos programinę įrangą ir perleido savo įrenginio ir operacijų elektroninės banki-ninkystės paskyros valdymą.

4 Kibernetiniai nusikaltimai siaurąja prasme

Nusikaltimai elektroninėje erdvėje siaurąja prasme – tai nusikaltimai, tiesiogiai darantys įtaką elektroninių duomenų ir informacinių sistemų saugumui, kitaip tariant, pati kompiuterinė sistema yra nusikaltimo tikslas.

IRD prie LR VRM duomenimis, 2022 m. šalyje užregistruota 919 elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų (LR BK 196–198² str.), tai sudarė apie 2 proc. visų užregistruotų nusikalstamų veikų, kaip ir 2021 m. 2021 m. šių nusikaltimų užregistruota 707, arba 212 mažiau (30 proc.), o jų ištyrimas siekė 48,1 proc. 2022 m. šių nusikaltimų ištyrimas sudarė 43,4 proc., t. y. 4,7 proc. mažiau nei 2021 m.

1 pav. >
2021–2022 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruotas elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų atvejų skaičius pagal LR BK 196–198² str.
(šaltinis – IRD prie LR VRM duomenys, FORMA_1G-IT)



Detalesnė informacija apie kiekvieną elektroninių duomenų ir informacinių išteklių saugumo nusikaltimą pagal LR BK 196–198² str.:

- ⚠ 196 str. „Neteisėtas poveikis elektroniniams duomenims“ – 2022 m. užregistruoti 22 nusikaltimai, t. y. 10 proc. daugiau nei 2021 m.
- ⚠ 197 str. „Neteisėtas poveikis informacinei sistemai“ – 2022 m. užregistruoti 3 nusikaltimai, t. y. 57,1 proc. mažiau nei 2021 m.
- ⚠ 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ – 2022 m. užregistruotas 51 nusikaltimas, t. y. 57,1 proc. mažiau nei 2021 m.

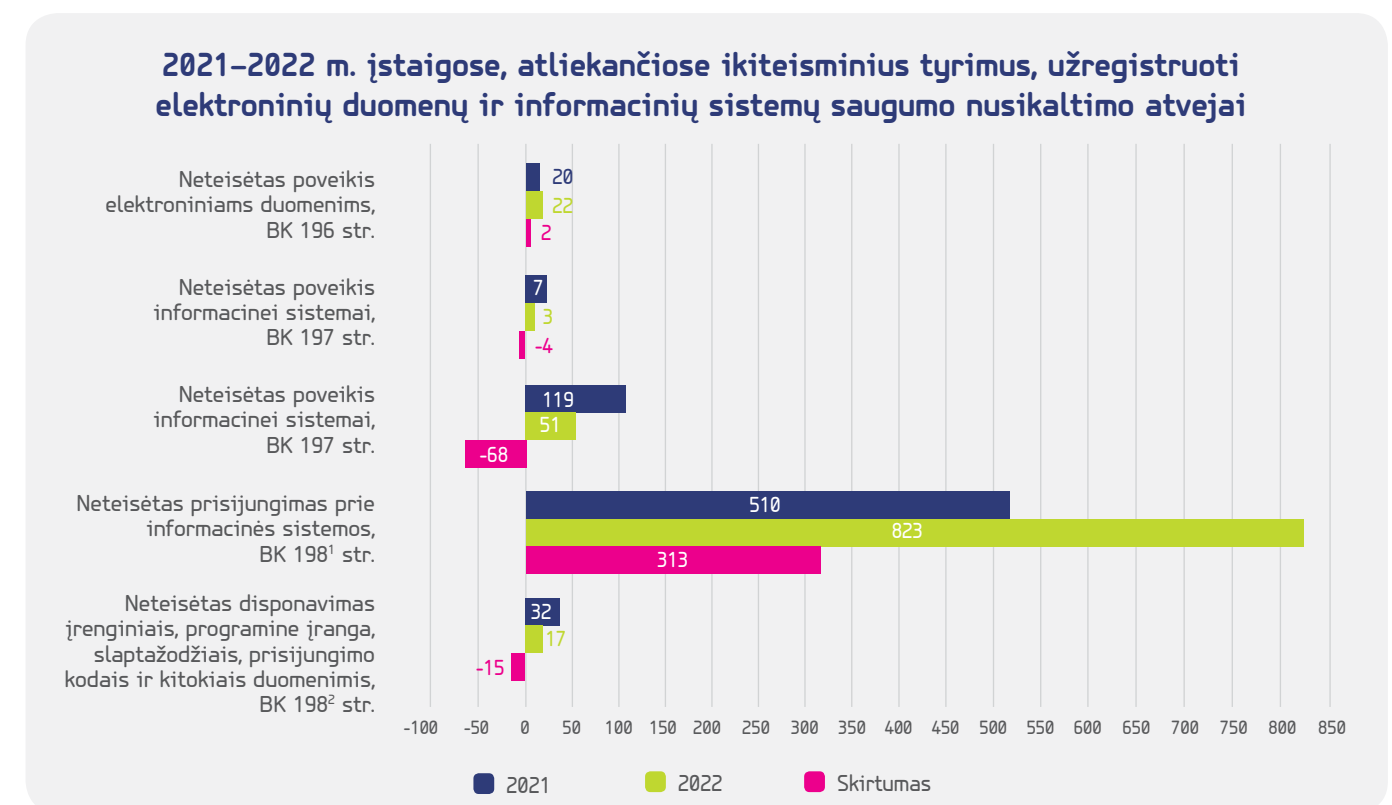
- ⚠ BK 198¹ str. „Neteisėtas prisijungimas prie informacinės sistemos“ – 2022 m. užregistruoti 823 nusikaltimai, t. y. 61,4 proc. daugiau nei 2021 m.
- ⚠ 198² str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis“ – 2022 m. užregistruota 17 nusikaltimų, t. y. 46,9 proc. mažiau nei 2021 m.

2022 m. kibernetiniai nusikaltimai siaurąja prasme nepasižymėjo rizikingomis būklės lygio tendencijomis. 2022 m. nežymiai padaugėjo kibernetinio chuliganizmo atvejų (+10 nusikalstamų veikų, arba 32 proc. daugiau nei 2021 m.) ir kibernetiniais būdais sprendžiamų buitinių konfliktų (+3 nusikalstamos veikos, arba 17 proc. daugiau nei 2021 m.). 2022 m. kibernetinio chuliganizmo atvejai reikiasi kaip poveikis informacinėms sistemoms ir (ar) jų duomenims neturint apibrėžtų motyvų (55 proc.) ir kaip akademinio jaunimo kibernetinis chuliganizmas siekiant ugdymo informacinėse sistemose platinti neetišką turinį ir (ar) trikdyti pamokas (45 proc.).

Palyginti su 2021 m., 2022 m. gerokai sumažėjo kibernetinių nusikaltimų, kurių motyvas buvo duomenų apie informacinių sistemų pažeidžiamumą ieškojimas ir (ar) elektroninių duomenų grobimas (-20 nusikalstamų veikų, arba 48 proc. mažiau nei 2021 m.). Beveik panašus išliko žmonių bauginimo ir (ar) terorizavimas kibernetiniais būdais atvejų skaičius (-2 nusikalstamos veikos, arba 13 proc. mažiau nei 2021 m.). Reikšmingais rodikliais taip pat nepasižymėjo prekyba pagrobtais informacinių sistemų vartotojų tapatybės ir autentifikavimo duomenimis, nors 2021 m. šie kibernetiniai nusikaltimai buvo naujas ir dinamiškiausias reiškinys iš savanaudiškais motyvais padarytų kibernetinių nusikaltimų (siaurąja prasme).

2022 m. iš kibernetinių nusikaltimų, kurių motyvas buvo duomenų apie informacinių sistemų pažeidžiamumą ieškojimas ir (ar) elektroninių duomenų grobimas, dominavo informacinių sistemų vartotojų tapatybės ir autentifikavimo duomenų vagystės (80 proc.). Šiems nusikaltimams įvykdyti pasirinktos tokios pačios priemonės: kenkimo užklausų atakos, SPAM laiškai su virusais, kenkimo PJ, skirta informacinėms sistemoms nulausti, slaptažodžiams atspėti ir (ar) duomenims automatizuotai nutekinti.

2 pav.
2021–2022 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruotas elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų atvejų skaičius pagal LR BK 196–198² str.
(šaltinis – IRD prie LR VRM duomenys, FORMA_1G-IT)



2022 m. išliko teigiama tendencija, kad atvejų, kai buvo naudojamosi elektroninius duomenis užšifruojančiais išpirkos reikalaujančio kenkimo programinio kodo virusais (angl. *ransomware*) ar DDoS atakomis, dalis elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų struktūroje nėra didelė (20 atvejų per metus) ir neprogresuoja.



Duomenis šifruojantis kenkimo programinis kodas

2022 m. užregistruota 17 (arba tiek pat kiek 2021 m.) atvejų, kai elektroniniai duomenys buvo užšifruoti kenkimo programinio kodo virusais. Nuo 2020 m. kibernetinių nusikaltimų dinamika rodo, kad tokio pobūdžio atakos nepasižymi augančia rizika. 2022 m. išpirka už elektroninių duomenų iškodavimą reikalauja paliekant virusais užkrėstose informacinėse sistemose raštelius su išpirkos mokėjimo nurodymais (angl. *ransom note*). 2022 m. reikalautų išpirkų dydis buvo nuo 0,03 BTC (675 eurų) iki 1000 BTC (22 529 000 eurų). Dažniausiai nurodyta išpirką sumokėti kriptovaliutos piniginių adresu. Nustatyta, kad elektroniniams duomenims užšifruoti buvo naudojami 6 šeimų kenkimo programinio kodo virusai: MAKOP (MKP), DEADBOLT, MEDUSALOCKER/LOCKFILESKR, PHOBOS, GLOBEIMPOSTER-ALPHA666QQZ, RL8s.exe. 2022 m. išryškėjo nauja tendencija – įsilaužėliai vis dažniau derino duomenų grobimo ir duomenų užšifravimo atakas. Tokiais atvejais, kai reikalaujama išpirka, grasinama pavišinti duomenis, ir jie neretai pavišinami, jei įsilaužėliai išpirkos negauna.



DDoS atakų programinė įranga

2022 m. užregistruoti 3 (arba +1 nusikalstama veika nei 2021 m.) atvejai, kai informacinės sistemos trikdytos DDoS atakomis. Nuo 2020 m. matoma ilgalaikė kibernetinių nusikaltimų dinamikos tendencija rodo, kad DDoS atakos nepasižymi didėjančia rizika. 2022 m. nustatyta viena masinė DDoS ataka, kai nuo 2022 m. birželio 20 d. iki 2022 m. birželio 29 d. trikdytos ne mažiau kaip 137 Lietuvos valstybės institucijos ir verslo interneto svetainės. Atsakomybę už šias atakas prisiėmė su Rusijos žvalgyba siejama grupuotė „Killnet“. Kitas DDoS atakas lėmė buitinių konfliktų darbovietėje ir interneto žaidimų grupėje aplinkybės.

5 Kibernetinius nusikaltimus lėmusios aplinkybės ir kibernetinių nusikaltimų poveikio vertinimas

Naudojimasis informacinių sistemų funkcionalumo ar apsaugos spragomis

2022 m. galimybės daryti kibernetinius nusikaltimus beveik nekito ir buvo susijusios su informacinių sistemų vartotojų aplaidumu ar klaidomis informacinėse sistemose: informacinės sistemos administratoriaus aplaidumas, įrenginio ir (ar) prisijungimo duomenų prieinamumas, interneto svetainės pažeidžiamumas, skirtingose informacinėse sistemose vienodų prisijungimo ir slaptažodžių duomenų naudojimas, dvigubos autentifikacijos nepasirinkimas, nesudėtingų slaptažodžių sukūrimas ir (ar) jų laikymas informacinių sistemų atmintyje, klaidos programinėje įrangoje, uždaruose tinkluose neužtikrintas nuotolinės prieigos funkcionalumas.

Kibernetinių nusikaltimų poveikis fiziniams asmenims

2022 m. iš visų subjektų, patiriančių kibernetinių nusikaltimų poveikį, dažniausiai nukentėdavo fiziniai asmenys (87 proc.). 2022 m., be socialine inžinerija paremto sukčiavimo, fiziniai asmenys taip pat patirdavo žalą dėl poveikio socialinių tinklų (6 proc.), el. pašto (2 proc.), interneto svetainių (2 proc.), mobiliųjų programėlių paskyroms (2 proc.) ir asmeniniams kompiuteriams (1 proc.). 2022 m. dažniausia fiziniams asmenims padarytų kibernetinių nusikaltimų pasekmė buvo paskyrų perėmimas (37 proc.). Kitos dažnos pasekmės – neteisėtų finansinių operacijų, užvaldžius paskyras ir (ar) elektroninės bankininkystės duomenis, inicijavimas (23 proc.), duomenų stebėjimas ir (ar) pasisavinimas (20 proc.), apgaulingo turinio, įgijus prieigą prie paskyrų, platinimas (7 proc.), duomenų pakeitimas (4 proc.). 2022 m. kibernetinės atakos prieš fizinių asmenų informacines sistemas dažniausiai buvo orientuotos į finansinių instrumentų (37 proc.), informacinių sistemų vartotojų autentifikavimo (22 proc.) ir privačius asmeninius duomenis (22 proc.).



Kibernetinių nusikaltimų poveikis juridiniams asmenims

2022 m. iš visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, juridiniai asmenys sudarė 12 proc. 2022 m. iš juridinių asmenų, patyrusių kibernetinių atakų poveikį, dominavo prekybos subjektai (3 proc.). Kitos 2022 m. akivaizdžiau matomos kibernetinės atakos buvo prieš informatikos ar telekomunikacijos paslaugų subjektus, apdirbamosios pramonės subjektus ir transportavimo paslaugų subjektus. 2022 m. kibernetinių atakų prieš juridinių asmenų informacines sistemas dažniausi padariniai – ūkinės veiklos duomenų užšifravimas ar kitoks sugadinimas (29 proc.), taip pat el. pašto adreso pakeitimas ir susirašinėjimo perėmimas (25 proc.), duomenų stebėjimas ar pasisavinimas (19 proc.), duomenų pakeitimas (10 proc.).



Kibernetinių nusikaltimų poveikis viešųjų paslaugų subjektams

2022 m. užregistruotos 23 prieš viešųjų subjektų informacines sistemas nukreiptos kibernetinės atakos, tai sudarė 4 proc. visų kibernetinių nusikaltimų. Kibernetinių atakų prieš viešųjų subjektų informacines sistemas šiek tiek sumažėjo (-6 nusikalstamomis veikomis, arba 21 proc. mažiau). Kibernetinės atakos dažniausiai patyrė švietimo sektoriaus informacinės sistemos (14 nusikalstamų veikų, arba 46 proc. visų viešųjų subjektų informacinių sistemų). Kibernetinių atakų prieš švietimo sektoriaus informacinės sistemos gerokai padaugėjo (+8 nusikalstamų veikų, arba 57 proc. daugiau). 2022 m. išryškėjo nauja tendencija – kibernetinės atakos prieš žiniasklaidos informacines sistemas (2 naujos nusikalstamos veikos). Šiek tiek padaugėjo kibernetinių atakų prieš informacines sistemas, kurias valdo sveikatos paslaugų (+1 nusikalstama veika) ir kultūros (+1 nusikalstama veika) subjektai. Gerokai sumažėjo kibernetinių atakų prieš aukštųjų mokyklų informacines sistemas (-18 nusikalstamų veikų, arba 90 proc. mažiau). Kibernetinėmis atakomis prieš viešųjų subjektų informacines sistemas dažniausiai buvo taikytasi į mokyklų elektroninį dienyną TAMO ir platintas apgaulingas ir (ar) žalingas turinys (13 nusikalstamų veikų, arba 35 proc.). Kitais kibernetinių nusikaltimų atvejais buvo siekiama pakenkti tarnybinei ir (ar) profesinei informacijai (7 nusikalstamos veikos, arba 19 proc.), platinti kenksmingą turinį (4 nusikalstamos veikos, arba 11 proc.), perimti paskyras socialiniuose tinkluose (3 nusikalstamos veikos, arba 8 proc.), pakenkti informacinių sistemų administravimo (2 nusikalstamos veikos, arba 6 proc.) ir ūkinės veiklos duomenims (2 nusikalstamos veikos, arba 5 proc.).





Kibernetinių nusikaltimų poveikis valstybės subjektams

2022 m. kibernetinės atakos prieš valstybės informacines sistemas nebuvo sistemingas reiškinys, užregistruota tik 1 nusikalstama veika (arba iki 1 proc.) – kibernetinė ataka prieš valstybės informacines sistemas, t. y. gerokai mažiau nei 2021 m. (-6 nusikalstamos veikos, arba 86 proc. mažiau nei 2021 m.). Iš viso per 2022 m. kibernetines atakas patyrė 6 valstybės sektoriai – po 1 kibernetinę ataką informacinės sistemos, kurias valdo centrinės valdžios, teismų, ministerijų, nacionalinio saugumo ir teisėsaugos, kariuomenės, savivaldybių subjektai.

2022 m. kibernetinės atakos prieš valstybės informacines sistemas nesukėlė valstybės ir tarnybos paslapčių pagrobimo padarinių. Užregistruota 1 kibernetinė plataus masto DDoS ataka prieš valstybės ir verslo subjektų interneto svetaines, iš kurių 19 valstybės subjektų (minėti anksčiau) administruojamų interneto svetainių.

6 Naudojamos prevencinės priemonės

2022 m. Lietuvos policija, įgyvendindama nustatytus nusikalstamumo kontrolės prioritetus, sistemingai vykdė prevencines priemones, kuriomis visuomenę informavo, kaip netapti sukčiavimo auka. Lietuvos policijos įstaigos savo prižiūrimos teritorijos gyventojus nuolat informavo apie dažniausius sukčiavimo būdus, teikė bendrą informaciją apie sukčiavimą, supažindino su naujausiomis kibernetinėmis grėsmėmis, mokė atpažinti socialinės inžinerijos atakas. Prevencinės priemonės buvo aktyviai vykdomos per socialinį tinklą „Facebook“, vietinę spaudą, lankstinukus (prekybos centruose, automobilių stovėjimo aikštelėse, renginiuose), el. paštu (daugiabučių namų savininkų bendrijų gyventojams), pamaldose (per šventikus), per virtualių pokalbių grupes, skirtas kaimiškųjų vietovių gyventojams, taip pat per susitikimus su seniūnais, pranešimus ir paskaitas mokymo įstaigose, susitikimuose su visuomene. Per 2022 m. bendruomenės pareigūnai turėjo 3 592 susitikimus visuomenės švietimo, kaip saugiai pirkti elektroninėje erdvėje, kaip apsaugoti nuo sukčiavimo elektroninėje erdvėje, taip pat lengvo uždario ir investavimo pavojų elektroninėje erdvėje prevencijos temomis. Susitikimuose dalyvavo 102 506 prižiūrimos teritorijos gyventojai. 2022 m. bendruomenės pareigūnai informaciją apie nusikaltimus „Facebook“ erdvėje viešino 1 784 kartus, skelbė mokyklų elektroniniuose dienynuose ir socialiniuose tinkluose, dalijosi prevenciniais patarimais.

Virtualus policijos patrulis savo „Facebook“ paskyroje skelbia prevencinius pranešimus, siekdamas įspėti interneto naudotojus apie gresiančius pavojus dėl galimo sukčiavimo bei svarbių asmens bei kitų duomenų vagysčių elektroninėje erdvėje (per 2022 m. paskelbti 25 pranešimai). „Facebook“ paskyroje privačiomis žinutėmis asmenys konsultuojami, ką daryti nukentėjus ir patyrus žalą elektroninėje erdvėje, taip pat virtualus patrulis, pastebėjęs socialiniuose tinkluose asmenis, kurie savo pasisakymais galimai peržengia įstatymo ribą, juos oficialiai įspėja dėl gresiančių pasekmių, o jiems veiksmų nenutraukus surenkama medžiaga ir perduodama atitinkamoms policijos įstaigoms.

2022 m. policijos virtualus patrulis pradėjo bendradarbiauti su Lietuvoje veikiančių skelbimų portalų administracija, susitarta dėl informacijos apsikeitimo pastebėjus galimus sukčiavimo atvejus. Nustatytos 42 internetinės svetainės, sukurtos siekiant apgaule išgauti asmenų banko sąskaitų duomenis. Su virtualaus patrulio pagalba svetainės užblokuotos ir pranešta serverių administratoriams. Identifikuota 15 atvejų, kai per dvi savaites vieno asmens padaryti ne mažiau nei penki

teisės pažeidimai elektroninėje erdvėje, taip pat nustatyta, kad mažiausiai 10 banko sąskaitų, naudojamų sukčiavimo tikslais, informacija buvo perduota teritorinėms policijos įstaigoms aplinkybėms toliau tikslinti. Užfiksuoti 3 atvejai elektroninėje erdvėje, galimai susiję su nepilnamečių išnaudojimu pornografijai, ir pradėti ikiteisminiai tyrimai. Iš viso per 2022 m. policijos virtualus patrulis nustatė ir užregistravo 349 galimus teisės pažeidimus, iš kurių dėl 30 pradėti ikiteisminiai tyrimai, dėl 227 – administracinio nusižengimo bylų teisenos.

Tobulėjant ir nuolat kintant sukčiavimo metodams ypač svarbus teisėsaugos bendradarbiavimas su privačiu sektoriumi, todėl svarų indėlį į sukčiavimo užkardymą turi 2021 m. gegužės mėn. pradėjusi veikti VŠĮ Pinigų plovimo prevencijos kompetencijų centras (toliau – AML centras), kurį įsteigė Lietuvos Respublikos finansų ministerija, Lietuvos bankas ir 8 šalyje veikiantys komerciniai bankai. AML centre įsteigta taktinio bendradarbiavimo grupė, joje dalyvaujantys finansų, kredito įstaigų ir teisėsaugos institucijų specialistai keičiasi aktualia informacija dėl finansinių sukčiavimų ir jų prevencijos. 2022 m. sausio 12 d. Lietuvos Respublikos vidaus reikalų ministerija, Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Finansinių nusikaltimų tyrimo tarnyba ir AML centro pasirašė bendradarbiavimo sutartį. Remiantis sutartimi keičiamasi informacija apie naujus sukčiavimų tipus bei taikomas ir planuojamas taikyti prevencines priemones, tobulinama finansų ir kredito įstaigų, teisėsaugos specialistų kvalifikacija kovos su sukčiavimu ir pinigų plovimu srityse.

Institucijoms bendradarbiaujant AML centro veikloje nuolat keičiamasi informacija apie situaciją, susijusią su sukčiavimais, jų tipus, dominavimu. Paminėtina, kad:

- ✓ remiantis finansų įstaigų ir policijos duomenimis, sudarytas nukentėjusiųjų profilis ir pradėta tikslinė vartotojų sąmoningumo kėlimo ir viešinimo kampanija;
- ✓ pagal sukauptą informaciją bankai pritaikė papildomas kontrolės priemones potencialiems sukčiams nustatyti;
- ✓ du didieji bankai įdiegė greitąjį pranešimo apie sukčiavimo atvejus mygtuką;
- ✓ Lietuvos kriminalinės policijos biuras sutarė su bankais ir išplatino aplinkraštį teritorinėms policijos įstaigoms dėl finansų įstaigų informavimo apie sąskaitų numerius, jų blokavimo, siekiant išvengti sisteminių sukčiavimų, susijusių su apgaulingais skelbimais dėl parduodamų prekių;
- ✓ AML centro taktinio bendradarbiavimo grupėje dalyvaujantys bankai pasidalijo kontaktais, kuriais, esant skubioms situacijoms, kai padaryta didelė žala ir yra nors kokia galimybė sustabdyti lėšas, galima kreiptis dėl lėšų sustabdymo.

Lietuvos policija nuolat ieško būdų tobulėti. Siekdama šio tikslo rengia įvairius mokymus, įskaitant ir nuotolinius, kuriuos darbuotojai gali išklausti mažesnio darbo krūvio metu ar atsiradus poreikiui neatidėliotinai įgyti naujų žinių. Kriminalinės policijos mokymų centras siūlo kursus sukčiavimo elektroninėje erdvėje prevencijos ir kitomis susijusiomis temomis.



ADSP ir jų prevencijos priemonių apžvalga



Dijana Šinkūnienė,
VDAI direktorė

Vadovo žodis

VDAI, kaip viena iš institucijų, įgyvendinančių kibernetinio saugumo politiką Lietuvoje, 2022 m. prisidėjo prie šios sistemos užtikrinimo: dalyvavo Kibernetinio saugumo tarybos veikloje, kibernetinio saugumo pratybose, bendradarbiavo tiriant kibernetinius incidentus.

Įgyvendindama vieną iš 2022 m. veiklos prioritetų stiprinti duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinias, kompetenciją ir įgūdžius asmens duomenų apsaugos srityje, VDAI sutelkė dėmesį į kibernetinio saugumo temą. Speciali kibernetinio saugumo dalis pristatyta 20 informuotumo skatinimo projekto „SolPriPa 2 WORK“ mokymų, skaityti pranešimai projekto uždarymo bei duomenų apsaugos pareigūnų ir organizacijų vadovų mokymuose, kad organizacijos dar kartą atkreiptų dėmesį, jog rūpintis kibernetiniu saugumu svarbu ne tik siekiant tinkamai apsaugoti asmens duomenis, bet ir užtikrinti organizacijos veiklos tęstinumą.



KA SAUGO?

- ✓ Žmogaus teisę į asmens duomenų apsaugą.



NUO KO SAUGO?

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



KAIP SAUGO?

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



VALSTYBINĖ
DUOMENŲ
APSAUGOS
INSPEKCIJA

1 Asmens duomenų apsaugos sąlygų lygis

Visų ES valstybių narių asmens duomenų apsaugos priežiūros institucijas vienijančios Europos duomenų apsaugos valdybos (toliau – EDAV) teigimu, per beveik penkerius Bendrojo duomenų apsaugos reglamento (toliau – BDAR) taikymo metus, visos įmonės, kurios netinkamai tvarkė klientų asmens duomenis iki BDAR, buvo išaiškintos ir nubaustos.

Nuo 2021 m. VDAI skaičiuoja ir vertina asmens duomenų apsaugos sąlygų lygį (toliau – ADASL) Lietuvoje. Lietuvoje 2022 m. ADASL⁰¹, palyginti su 2021 m., nesikeitė ir siekė 60 proc. (ADASL siektina vertė yra 100 proc.). VDAI nuomone, šis rodiklis išliko stabilus, atsižvelgiant į tai, kad 2022 m. Lietuvoje nevyko reikšmingų pokyčių ar įvykių, susijusių su asmens duomenų apsauga.

ADASL yra sudėtinis rodiklis, nustatomas pagal 10 klausimų iš kasmet atliekamos reprezentatyvios Lietuvos gyventojų apklausos. Klausimai apima keturias sritis: gyventojų žinias, pasitikėjimą įmonėmis ir įstaigomis dėl asmens duomenų tvarkymo, elgesį susidūrus su pažeidimais ir pasitikėjimą priežiūros sistema.

Remiantis apklausos duomenimis, 2022 m. gyventojai rečiau susidūrė su ADSP. Maždaug 72 proc. gyventojų teigia, kad per pastaruosius metus nesusidūrė su jokių neteisėtų jų asmens duomenų tvarkymu, t. y. 5 proc. daugiau gyventojų negu 2021 m. Visgi padaugėjo gyventojų, kurie susidūrė su ADSP kreiptųsi į atsakingą priežiūros instituciją (atsakymų dalis „labai tikėtina“ – 24 proc. 2022 m., tai 5 proc. daugiau negu 2021 m.). Dauguma apklaustųjų (54 proc.) pasitiki valstybės institucijomis, kurios prižiūri, ar kitos įmonės, įstaigos ar kitos organizacijos tinkamai užtikrina asmens duomenų apsaugą.

2 ADSP Lietuvoje situacijos analizė

VDAI pastebi, kad 2022 m., kaip ir anksčiau, nemažai ADSP sudarė duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *ransomware*). Duomenų valdytojai patyrė gana didelę žalą, turėjo šių ADSP suvaldymui ir žalos bei poveikio sumažinimui skirti daug finansinių ir žmogiškųjų išteklių. Piktavaliai taikydami įvairius socialinės inžinerijos ir duomenų viliojimo (angl. *phishing*) metodus, pasitelkdami gerai apgalvotus scenarijus ir įvairius ryšio užmezgimo kanalus siekė gauti įvairius prisijungimo duomenis.

2022 m. pastebėtos ir tiekimo grandinės atakos (angl. *supply chain attack*) – organizacijos duomenų saugumui grėsmė kildavo per trečiųjų šalių paslaugų teikėjus ir jų tiekiamą programinę įrangą ar jos komponentus. Taigi, didėja naudojamos programinės ir techninės įrangos gamintojų ar debesijos paslaugų teikėjų patikimumo, reputacijos ir kilmės šalies įvertinimo ir potencialių rizikų duomenų saugumui nustatymo svarba.

Taip pat išryškėjo spragos prieigos kontrolės valdymo organizacijų kompiuterių tinkluose – suteikiant prieigą netaikomi apribojimai ir tinklo segmentavimas, nesilaikoma „mažiausių teisių privilegijos“ ir „būtinių žinoti“ principų, netaikomas dviejų ir daugiau veiksmų autentifikavimas (angl. *2 factor authentication*, 2FA) aukštesnes teises turintiems ar nuotoliniu būdu besijungiantiems (pavyzdžiui, per

⁰¹

ADASL 2022 m., https://vdai.lrv.lt/uploads/vdai/documents/files/2022%20m_%20ADASL_ataskaita.pdf.

nuotolinio darbalaukio protokolą (angl. *Remote Desktop Protocol*, RDP) ar virtualų privatų tinklą (angl. *Virtual Private Network*, VPN) naudojančiams vartotojams.

VDAI atkreipė dėmesį, kad įgyvendinant duomenų valdytojų ir tvarkytojų atskaitomybės principą bei siekiant tinkamai suvaldyti ir iširti ADSP, būtina ne tik kaupti ir saugoti žurnalų įrašus (angl. *logs*), bet ir apsaugoti juos nuo sunaikinimo ar užšifravimo ADSP atveju bei turėti galimybę nuolat ir centralizuotai juos apdoroti, saugoti ir analizuoti. Praradus atakuojamus žurnalų įrašus nebelieka galimybės patikimai nustatyti įvykdytų atakų vektorių ir piktavalių atliktų neteisėtų veiksmų su duomenimis bei tinkamai nustatyti piktavalių išnaudotų saugumo spragų ir jo veiksmų sekos ir laiko.

Daugėja ADSP atvejų, kai piktavaliai surengia gerai apgalvotas, įmantrias ir ilgą laiką trunkančias kibernetines atakas. Atakos pasižymi aukštu techniniu pasirengimu, kintančiomis kryptimis, gebėjimu prisitaikyti prie kintančios situacijos ir organizacijos atliekamų gynybinio pobūdžio veiksmų. Duomenų valdytojai turėtų rimtai vertinti duomenų saugumo iššūkius, turėti už duomenų saugumo užtikrinimą ir reagavimą į ADSP atsakingus asmenis ar paslaugų teikėjus bei skirti tam pakankamą finansavimą ir kitus būtinus išteklius.

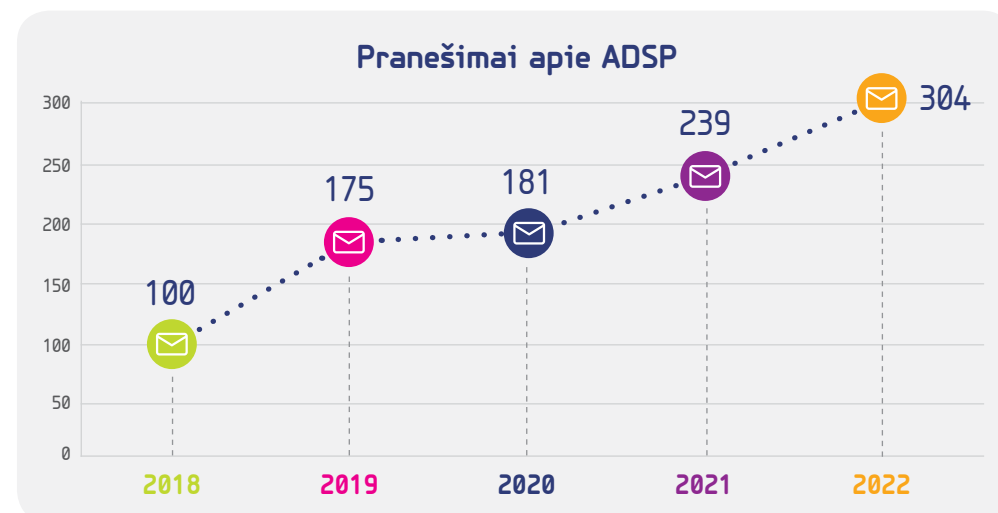
Rusijos karas Ukrainoje sukėlė dar didesnę kibernetinių atakų bangą ir pablogino kibernetinio saugumo situaciją pasaulyje. Nors Rusijos karo kontekste VDAI specialių priemonių nerengė, tačiau dėl padidėjusios grėsmės organizacijų tvarkomiems asmens duomenims bendraudama su duomenų valdytojais ir tvarkytojais bei rengdama įvairias informuotumo skatinimo priemones pabrėžė būtinybę dar daugiau dėmesio skirti tinkamoms techninėms ir organizacinėms asmens duomenų tvarkymo priemonėms. Duomenų valdytojams ir tvarkytojams ypač svarbu laiku užtikrinti pažeidžiamumą ir atnaujinimų valdymą. Jie turėtų imtis aktyvių veiksmų, kurie padėtų apsaugoti:

- ✓ naujai įvertinti kylančias grėsmes ir rizikas jų duomenų saugumui ir sparčiau diegti gamintojų išleidžiamus programinės ir aparatinės įrangos (angl. *firmware*) atnaujinimus;
- ✓ stropiai laikytis gamintojų nurodomų saugumo užtikrinimo nuostatų ir gerosios jų įgyvendinimo praktikos;
- ✓ sekti informaciją internete apie jų naudojamos programinės įrangos pažeidžiamumus, ypač jei jie aktyviai išnaudojami, ir nedelsdami imtis priemonių saugumo spragoms pašalinti.

VDAI gaunamų pranešimų apie ADSP kasmet daugėja (2018 m. – 100, 2019 m. – 175, 2020 m. – 181, 2021 m. – 239, 2022 m. – 304), tačiau priežiūros institucija tai sietų ne su pačių pažeidimų gausėjimu, o su duomenų valdytojų įgyjamų žinių, sąmoningumo asmens duomenų apsaugos srityje didėjimu, suvokimu, kas apskritai yra laikoma ADSP ir kokių veiksmų turi imtis organizacijos jiems įvykus.

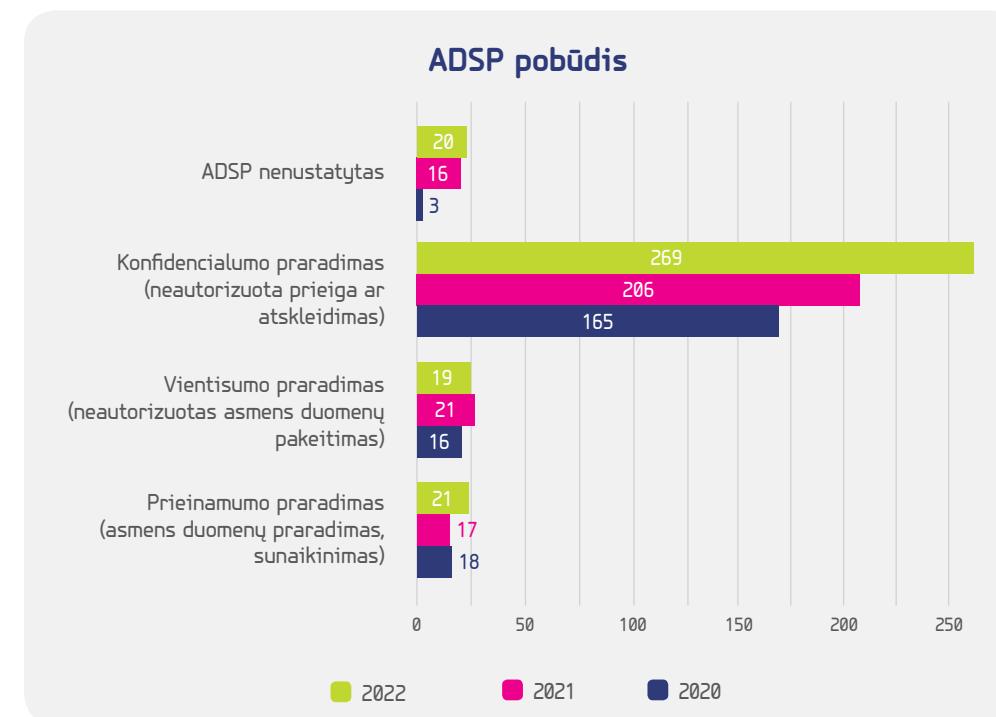
1 pav. >

Pranešimų apie ADSP dinamika 2018–2022 m. (šaltinis – VDAI)



< 2 pav.

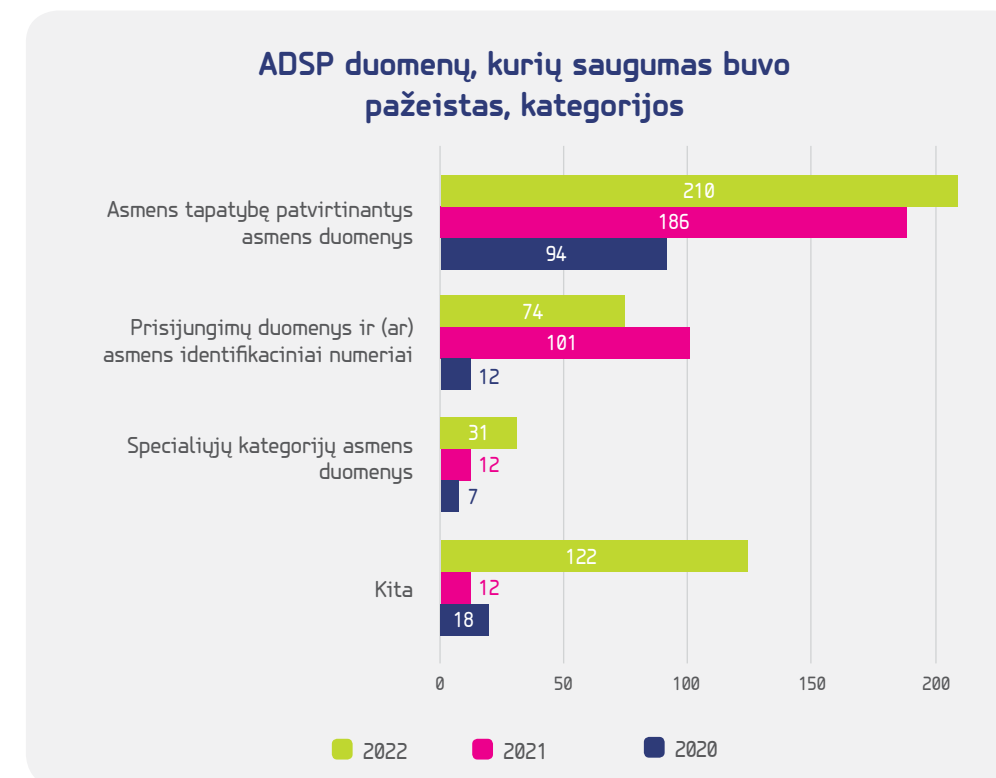
ADSP pobūdis 2020–2022 m. (šaltinis – VDAI)



Pagal ADSP pobūdį (gali būti daugiau negu vienas požymis) Lietuvoje statistiškai neabejotinai vyrauja konfidencialumo pažeidimai – 2022 m. net 269 atvejais buvo prarastas asmens duomenų konfidencialumas. 21 ADSP buvo susijęs su duomenų prieinamumo pažeidimais, 19 – prarastu duomenų vientisumu.

< 3 pav.

ADSP duomenų, kurių saugumas buvo pažeistas, kategorijos 2020–2022 m. (šaltinis – VDAI)

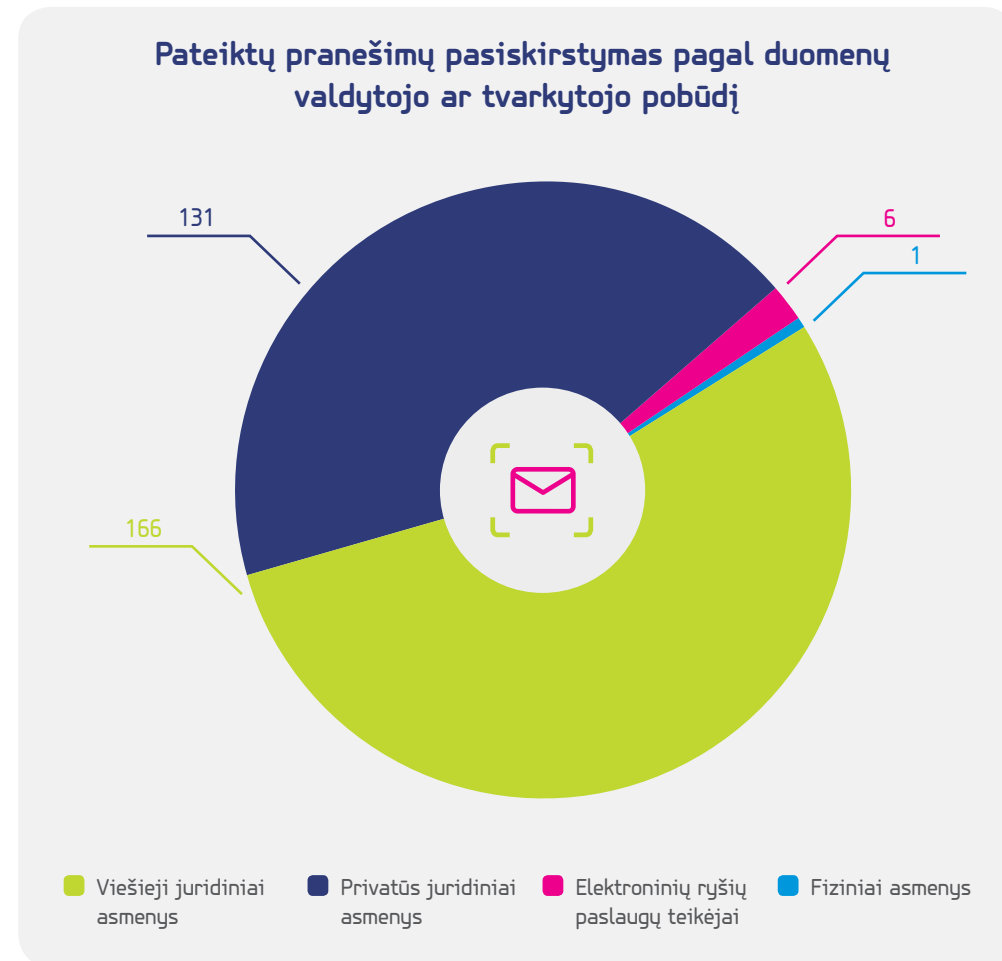


Asmens duomenų, kurių saugumas buvo pažeistas, kategorijose vyrauja „Asmens tapatybę, patvirtinantys asmens duomenys“ – iš viso nustatyta 210 atvejų, „Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai“ – 74 atvejai. Šių kategorijų asmens duomenys dažniausiai buvo naudojami neteisėtai prieigai prie informacinių sistemų, interneto svetainių ir tolesnei neteisėtai veiklai vykdyti,

pavyzdžiui, kenkimo PĮ platinimui, sukčiavimui, susijusiam su el. prekyba ar pinigų pervedimu ir pan. „Specialių kategorijų asmens duomenų“ pažeidimai sudarė 31 atvejį, 122 kartus pažeistų duomenų kategorija buvo nurodyta kaip „Kita“.

4 pav. >

Pateiktų pranešimų pasiskirstymas pagal duomenų valdytojo ar tvarkytojo pobūdį (šaltinis – VDAI)



02

VDAI sprendimas dėl IT bendrovės negebėjimo užtikrinti nuolatinio duomenų tvarkymo sistemų ir paslaugų konfidencialumo, vientisumo, prieinamumo ir atsparumo, <https://vdai.lrv.lt/uploads/vdai/documents/files/2022-05-02%20Sprendimas%20ADSP%2C%20saugumo%20priemoniu%20neuztikrinimas.pdf>.

2022 m. VDAI skyrė 2 administracines baudas dėl bendrovėse įvykusių ADSP



2022 m. kovo mėn. VDAI priėmė sprendimą skirti 3 tūkst. eurų baudą vienai iš Lietuvoje veikiančių kolegijų dėl duomenų tvarkymo saugumo pažeidimo, t. y. negebėjimo užtikrinti nuolatinio duomenų tvarkymo sistemų ir paslaugų konfidencialumo, vientisumo, prieinamumo ir atsparumo bei netinkamo techninių ir organizacinių priemonių taikymo (BDAR 32 straipsnio 1 dalies b ir d punktų pažeidimas).



2022 m. gegužės mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą informacinių technologijų (toliau – IT) bendrovei skirti 35 tūkst. eurų baudą⁰² už nustatytus BDAR nuostatų pažeidimus. Per incidentą buvo pažeistas daugiau kaip 130 tūkst. duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. VDAI nustatė, kad pasinaudojus IT bendrovės darbuotojo paskyros prisijungimo prie elektroninės parduotuvės valdymo skydelio duomenimis ir per išorinį tinklą prisijungus prie elektroninės parduotuvės įkelta kenkimo rinkmena (.gif) ir serveris užkrėstas virusu bei nutekinti IT bendrovės klientų duomenys. ADSP įvyko dėl neįgyvendintos organizacinės ir techninės saugumo priemonės prieigų kontrolės ir autentifikavimo, darbo stočių ir tinklo saugos srityse, t. y. IT bendrovė, neužtikrindama tinkamos prieigos kontrolės ir vartotojų autentifikacijos, tinkamos darbo stočių apsaugos, nefiksuodama ir nekaupdama techninių žurnalų įrašų, leidžiančių identifikuoti ir stebėti, sekti naudotojų veiksmus, sudarė sąlygas tretiesiems asmenims be autorizacijos pasiekti IT bendrovės klientų duomenis. Buvo pažeisti BDAR 32 straipsnio 1 dalies b punkto reikalavimai, kurie įpareigoja organizaciją užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą.

3 Tarptautinio bendradarbiavimo iniciatyvos ir mokymo bei švietimo veiklos

BDAR įtvirtintas privalomas nacionalinių asmens duomenų apsaugos priežiūros institucijų indėlis į EDAV ir jos pogrupių veiklą. VDAI vykdo aktyvią tarptautinę veiklą EDAV ir bendradarbiavimą su kitų valstybių narių priežiūros institucijomis atliekant tikrinimus ir sprendžiant bylas, kurioms taikomas BDAR numatytas nuosekumo užtikrinimo mechanizmas, kai galimai netinkamai tvarkomi ne tik Lietuvos, bet ir kitų ES valstybių piliečių asmens duomenys.

Lietuva prisideda prie koordinuotų asmens duomenų apsaugos viešajam sektoriui naudojantis debesių paslaugomis tikrinimų. 2022 m. vasario mėn. EDAV vienijamos 22 nacionalinės asmens duomenų apsaugos priežiūros institucijos iš visos Europos ekonominės erdvės (EEE), įskaitant ir EDAV, pradėjo koordinuotus viešojo sektoriaus naudojimosi debesių paslaugomis tikrinimus⁰³. Remiantis EDAV surinkta informacija, pastaruosius šešerius metus organizacijų naudojimosi debesių paslaugomis mastas padvigubėjo. COVID-19 pandemija paskatino organizacijas pereiti prie skaitmeninių formatų. Debesijos technologijomis pradėjo naudotis ir daugybė viešojo sektoriaus organizacijų. Naudojantis šiomis paslaugomis tiek nacionaliniu, tiek ES lygmeniu neretai gali būti susiduriama su sunkumu gauti ES asmens duomenų apsaugos taisyklės atitinkančius informacinių ir ryšių technologijų produktus ir paslaugas. Vadovaudamasi suderintomis gairėmis ir atlikdamos koordinuotus veiksmus, asmens duomenų apsaugos priežiūros institucijos siekia skatinti geriausią praktiką ir užtikrinti tinkamą asmens duomenų apsaugą. VDAI taip pat dalyvauja šioje iniciatyvoje – Lietuvoje asmens duomenų apsaugos naudojantis debesių paslaugomis tikrinimas numatytas Lietuvos statistikos departamente (nuo 2023 m. sausio 1 d. – Valstybės duomenų agentūroje). Išvados bus pateiktos susipažinti visuomenei 2023 m.

Duomenų apsaugos pareigūnų mokymuose – speciali mokymų dalis organizacijų vadovams

2022 m. lapkričio mėn. VDAI surengė kasmetinius duomenų apsaugos pareigūnų mokymus⁰⁴. Pirmoji mokymų dalis buvo skirta viešojo bei privataus sektoriaus organizacijų vadovams. Viena iš pranešimų „Kibernetinio saugumo svarba ir santykis su asmens duomenų apsauga“ aptarti kibernetinio saugumo klausimai organizacijose. Mokymų įrašas buvo prieinamas visuomenei keletą savaičių ir sulaukė 4,3 tūkst. peržiūrų.

„SolPriPa 2 WORK“ projektas

2022 m. VDAI kartu su Mykolo Romerio universitetu tęsė dvejų metų trukmės darbuotojų ir darbdavių informuotumo apie asmens duomenų apsaugą skatinimo projektą⁰⁵ „Sprendžiant privatumo paradoksą 2: aukštų duomenų apsaugos, kaip pagrindinės teisės, standartų skatinimas darbo vietoje“. Įgyvendinant šį projektą, surengta 20 mokymų, iš jų 14 smulkiojo ir vidutinio verslo atstovams, 2 savivaldybėms, 2 teismams ir 2 ministerijoms, joms pavaldžioms ir kitoms viešojo sektoriaus institucijoms. Viena iš mokymų dalių buvo skirta asmens duomenų saugumo klausimams organizacijose aptarti ir galimiems sprendimams rasti. Taip pat sukurta 10 tinklalaidžių, parengti 3 moksliniai straipsniai, 3 gairės, surengta nuotolinė projekto uždarymo konferencija visuomenei ir atnaujinta mobilioji programėlė „ADA gidas“.

03

Lietuva prisidės prie koordinuotų asmens duomenų apsaugos viešajam sektoriui naudojantis debesių paslaugomis tikrinimų, <https://vdai.lrv.lt/lt/naujienos/lietuva-prisides-prie-koordinuotu-tikrinimu-del-asmens-duomenu-apsaugos-viesajam-sektoriui-naudojantis-debesijos-paslaugomis>.

04

Organizacijų vadovams ir duomenų apsaugos pareigūnams VDAI rengia mokymus aktualiais asmens duomenų apsaugos klausimais, <https://vdai.lrv.lt/lt/naujienos/organizaciju-vadovams-ir-duomenu-apsaugos-pareigunams-valstybine-duomenu-apsaugos-inspekcija-rengia-mokymus-aktualiais-asmens-duomenu-apsaugos-klausimais>.

05

Daugiau informacija apie „SolPriPa 2 WORK“ projektą <https://vdai.lrv.lt/lt/naudinga-informacija/solpripa-2-work-projektas>.



Priešiškos informacinės aplinkos apžvalga ir Lietuvos informacinės aplinkos saugumo vertinimas



Komandoras Giedrius Valintėlis,
LK SKD direktorius

Vadovo žodis

Lietuvos kariuomenės užduotis – ginklu ginti Lietuvos valstybę. Taikos metu Lietuvos kariuomenė vykdo nenutrūkstamą karinį rengimą, išlaikydama aukštą kovinę parengtį, kuri yra vienas iš pagrindinių potencialaus priešo atgrasymo nuo galimo ginkluoto konflikto su Lietuvos valstybės elementų. Tai turime aiškiai demonstruoti savo veiksmais, komunikacija ir siekti priešiškų auditorijų suvokimo, kad Lietuvos puliti neverta, nes pavojinga ir pražūtinga.

Lietuvos kariuomenės Strateginės komunikacijos departamentas analizuoja priešišką ir draugišką informacinę aplinką, stebi tendencijas ir temas, kurias plėtoja priešiškos jėgos, analizuoja informacinės aplinkos įtaką Lietuvos kariuomenės užduotims ir įvaizdžiui. Remdamasis analizės duomenimis gali teikti patarimus Lietuvos karinei vadovybei bei užtikrinti Lietuvos kariuomenės komunikacijos efektyvumą atitinkamoms auditorijoms.



KĄ SAUGO?

- ✓ Nacionalinę ir NATO informacinę aplinką.



NUO KO SAUGO?

- ✓ Nuo priešiškų organizacijų ir valstybių vykdomų informacinių operacijų.



KAIP SAUGO?

- ✓ Vertindamas informacinę aplinką, kartu su NKSC stebi ir analizuoja informacinius bei kibernetinius incidentus.
- ✓ Bendradarbiaudamas su valstybinėmis ir tarptautinėmis institucijomis, žiniasklaida bei nevyriausybėmis organizacijomis, padeda identifikuoti, užkardyti ir (ar) neutralizuoti informacines operacijas.
- ✓ Informuodamas visuomenę apie vykdomą manipuliaciją jos jausmais, įsitikinimais bei interesais, siekiant ją klaidinti.
- ✓ Siekdamas prevenciškai ir (ar) efektyviai mažinti prieš Lietuvos nacionalinio saugumo ir gynybos interesus nukreiptos informacijos padarinius, skatina visuomenę kritiškai mąstyti.
- ✓ Remdamas visuomenės pilietiškumo ugdymą, koordinuoja kariuomenės ir visuomenės bendradarbiavimą.



LIETUVOS KARIUOMENĖS
STRATEGINĖS KOMUNIKACIJOS
DEPARTAMENTAS



kariuomene.lt



info@mil.lt



8 618 26857

1 Informacinės aplinkos grėsmių tendencijos

Dėl Rusijos pradėtos karinės invazijos į Ukrainą 2022 m. informacinės konfrontacijos kontekste buvo išskirtiniai. Ypač daug dėmesio tiek Kremliaus, tiek Baltarusijos režimų kontroliuojami informacijos šaltiniai skyrė gynybos sektoriaus temoms:

- ⚠ NATO;
- ⚠ NATO pajėgumų stiprinimui Baltijos regione;
- ⚠ Lietuvos narystei NATO;
- ⚠ Lietuvos karinio potencialo stiprinimui.

Daug dėmesio taip pat buvo skiriama Lietuvos vykdomai užsienio politikai: dvišaliams ir daugiašaliams santykiams, narystei tarptautinėse organizacijose, paramai Ukrainai.

Informacinės operacijos vykdyti 2022 m. buvo pasitelktos pačios įvairiausios priemonės ir šiuolaikinės technologijos. Kaip įrankiu propagandai skleisti naudotasi Rusijos ir Baltarusijos valstybiniais bei Vakarų auditorijoms skirtais kontroliuojamais informacijos sklaidos kanalais, kibernetinės atakos vykdytos derinant su melagienų (angl. *fake news*) sklaida. Dažnu atveju priešiškos ir (ar) nedraugiškos informacinės veiklos skleidėjais 2022 m. tapdavo Rusijos ir Baltarusijos politikai, diplomatai, aukšto rango karininkai ir valstybės institucijų atstovai, taip pat tariami kariniai ar politiniai ekspertai. 2022 m. informaciniai incidentai prieš Lietuvą ir valstybės interesus dažniausiai buvo vykdomi per interneto naujienų portalus bei socialinius tinklus.

Politinį ir šalies saugumą stiprinančių procesų, kuriuose Lietuvos Respublika aktyviai dalyvavo arba kurie buvo tiesiogiai susiję su mūsų valstybe, gausa 2022 m. nulėmė ir didesnį neigiamą Rusijos bei Baltarusijos dėmesį Lietuvai. Priešiška informacinė veikla buvo susijusi su 2021 m. gruodžio 16 d. Lietuvos Respublikos Seimo atnaujintoje Nacionalinio saugumo strategijoje⁰¹ apibrėžtomis trimis strateginėmis sritimis: **(1) gynybos**; **(2) užsienio politikos** bei **(3) konstitucinių pagrindų apsaugos**. Dokumente pabrėžiama, kad „tarptautinė sistema tampa vis sunkiau prognozuojama dėl pastaraisiais metais išryškėjusių globalių ir regioninių procesų. Grėsmių kompleksiskumas pasižymi nykstančiomis skirtimis tarp karo ir taikos, išorinių ir vidinių, karinių ir nekarinių grėsmių, valstybinių ir nevalstybinių grėsmių šaltinių. Tai lemia didesnį hibridinių grėsmių iššūkį euroatlantinei bendruomenei, taigi ir Lietuvos Respublikai“.

Rusijos kariniai veiksmai prieš Ukrainą paskatino konsoliduoti ir lanksčiai pritaikyti LK SKD duomenų rinkimo, apdorojimo ir analizės pajėgumus. Buvo tęstas priešiškos Lietuvai informacinės aplinkos stebėjimas, analizė ir vertinimas, nustatyti Rusijos ir Baltarusijos skleidžiamos priešiškos informacijos pokyčiai, susiję su karo Ukrainoje pradžia. Apie pokyčius ir propagandos grėsmes buvo informuojamos valstybinės institucijos, užsienio partneriai, žiniasklaida, visuomenė.

LK SKD taip pat atskiroms institucijoms teikė informaciją apie informacinį spaudimą įvairiose srityse. Be to, siekdamas užtikrinti visuomenės ir valstybės informuotumą apie informacines grėsmes, LK SKD viešai atsakinėjo į žiniasklaidos atstovų pateiktus klausimus apie tendencijas priešiškoje informacinėje aplinkoje. LK SKD, siekdamas sumažinti Rusijos Federacijos propagandos poveikį

01

Nacionalinio saugumo strategija,
<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr>.

bei prisidėti prie visuomenės psichologinio stabilumo, nuolatos ir pagal poreikį informuodavo Lietuvos piliečius apie saugumo situaciją. LK SKD atstovai skaitė visuomenei paskaitas apie Rusijos vadovybės vykdomas informacines operacijas prieš Ukrainą, kartu parodydami jų ir Lietuvoje bei kitose Baltijos šalyse vykdomų informacinių operacijų panašumus bei skirtumus.

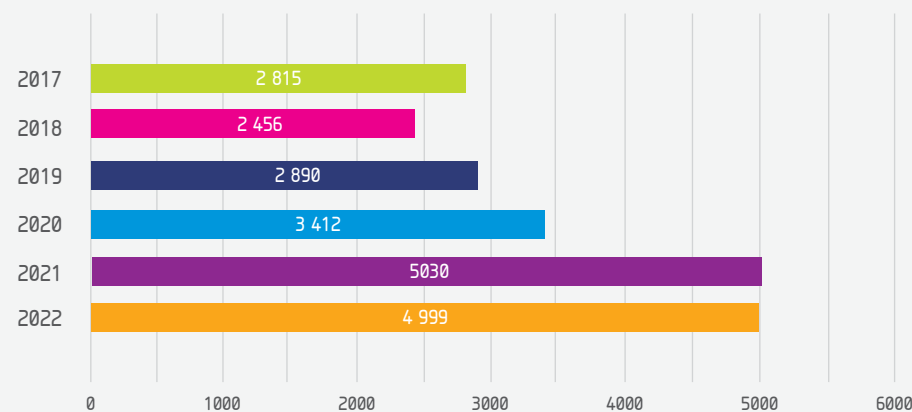
2 Prieš Lietuvos nacionalinius interesus vykdytos informacinės operacijos ir jų tendencijos

Bendras Lietuvai priešiškos informacinės veiklos atvejų skaičius 2022 m. sudarė **4 999** unikalius informacinius atvejus. Palyginti su pastarųjų penkerių metų duomenimis, informacinių incidentų skaičius nuosekliai augo, informacinis spaudimas Lietuvai ir kitoms Baltijos šalims tendencingai didėjo (žr. **1 pav.**).

1 pav. >

Unikalių priešiškos informacinės atvejų skaičius pagal metus
(šaltinis – LK SKD)

Unikalių priešiškos informacinės atvejų skaičius pagal metus

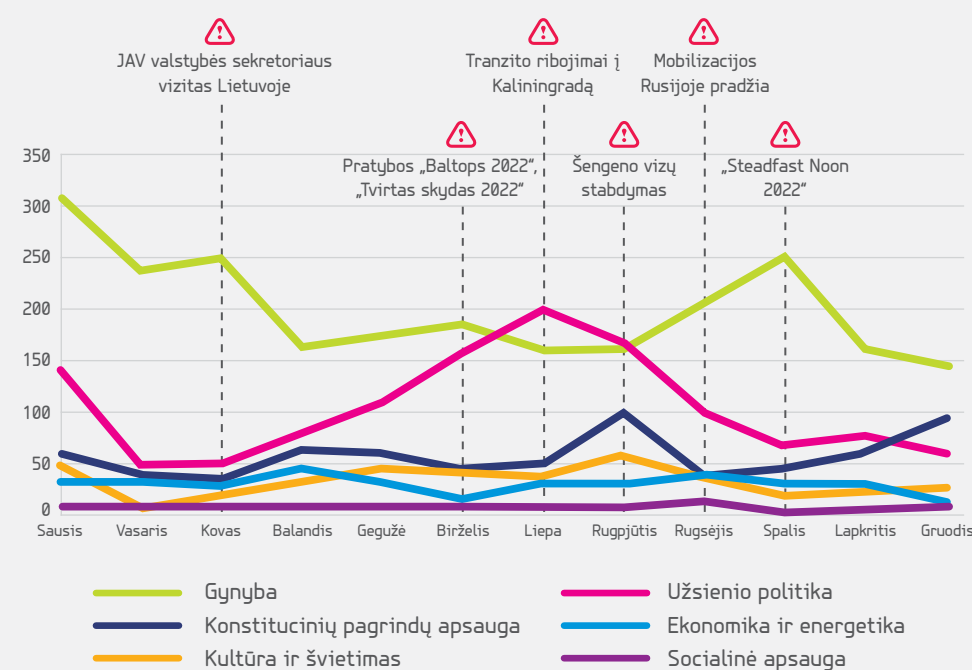


Tai lėmė šie 2022 m. svarbūs nacionalinės ir tarptautinės reikšmės įvykiai:

- JAV gynybos sekretoriaus Lloyd Austino vizitas Lietuvoje vasario 19 d.
- Rusijos karinės agresijos prieš Ukrainą pradžia vasario 24 d. ir nepaprastosios padėties įvedimas Lietuvoje.
- JAV valstybės sekretoriaus Antonio Blinkeno vizitas Lietuvoje kovo 7 d.
- Lietuvos Respublikos Seimo priimta rezoliucija dėl Rusijos pripažinimo terorizmu remiančia ir vykdančia valstybe gegužės 10 d.
- Suomijos ir Švedijos stojimo į NATO paraiškų oficialus pateikimas gegužės 18 d.
- Papildomų ribojimų kroviniui tranzitui į Kaliningradą įsigaliojimas Lietuvoje liepos 10 d.

- Lietuvos Respublikos užsienio reikalų ministerijos siūlymas nutraukti Šengeno vizų išdavimą Rusijos piliečiams rugpjūčio 16 d.
- Lietuvos kariuomenės infrastruktūros plėtra: trijų karinių miestelių statybos darbų pradžia rugpjūčio 24 d.
- „Nord Stream“ vamzdynų Baltijos jūroje incidentai rugsėjo 27–29 d.
- Tarptautinės NATO pratybos „Steadfast Noon 2022“ spalio 17–30 d.
- G20 viršūnių susitikimas Indonezijoje lapkričio 15–16 d.
- ES gynybos ministrų susitarimas dėl Ukrainos karių apmokymo misijos („EUMAM Ukraine“) lapkričio 15 d.
- NATO Parlamentinės Asamblėjos rezoliucija dėl Rusijos paskelbimo teroristine valstybe lapkričio 21 d.
- Europos Parlamento paskelbtas sprendimas pripažinti Rusiją terorizmą remiančia valstybe lapkričio 23 d.
- Krašto apsaugos ministro Arvydo Anušausko susitikimas su JAV gynybos sekretoriumi Lloyd Austinu ir sutarties dėl didelio mobilumo raketinės artilerijos sistemos HIMARS įsigijimo sudarymas gruodžio 14–17 d.
- Ukrainos prezidento Volodymyro Zelenskio vizitas į JAV, susitikimas su JAV prezidentu Joe Bidenu gruodžio 21 d.
- ES sankcijos Rusijai (patvirtinti 9 sankcijų paketai).

Informacinio spaudimo dinamika 2022 m.



< 2 pav.

2022 m. priešiškos informacinės veiklos koreliacija su nacionalinėmis sritimis (gynyba, užsienio politika, ekonomika ir energetika, kultūra ir švietimu, konstitucinių pagrindų apsauga, socialinė apsauga) ir įvykiais (šaltinis — LK SKD)

Priešiškos informacijos atvejų intensyvumui 2022 m. buvo būdinga sričių tarpusavio koreliacija. Gynybos sritis buvo veikiamą ne tik tiesiogiai, bet ir (ar) netiesiogiai per kitas sritis. 2022 m. tarpusavyje daugiausia koreliavo gynybos, užsienio politikos, konstitucinių pagrindų apsaugos bei ekonomikos ir energetikos sritys. Šių temų tarpusavio koreliacijos atspindėjo priešiškos komunikacijos daugiasluoksniškumą.

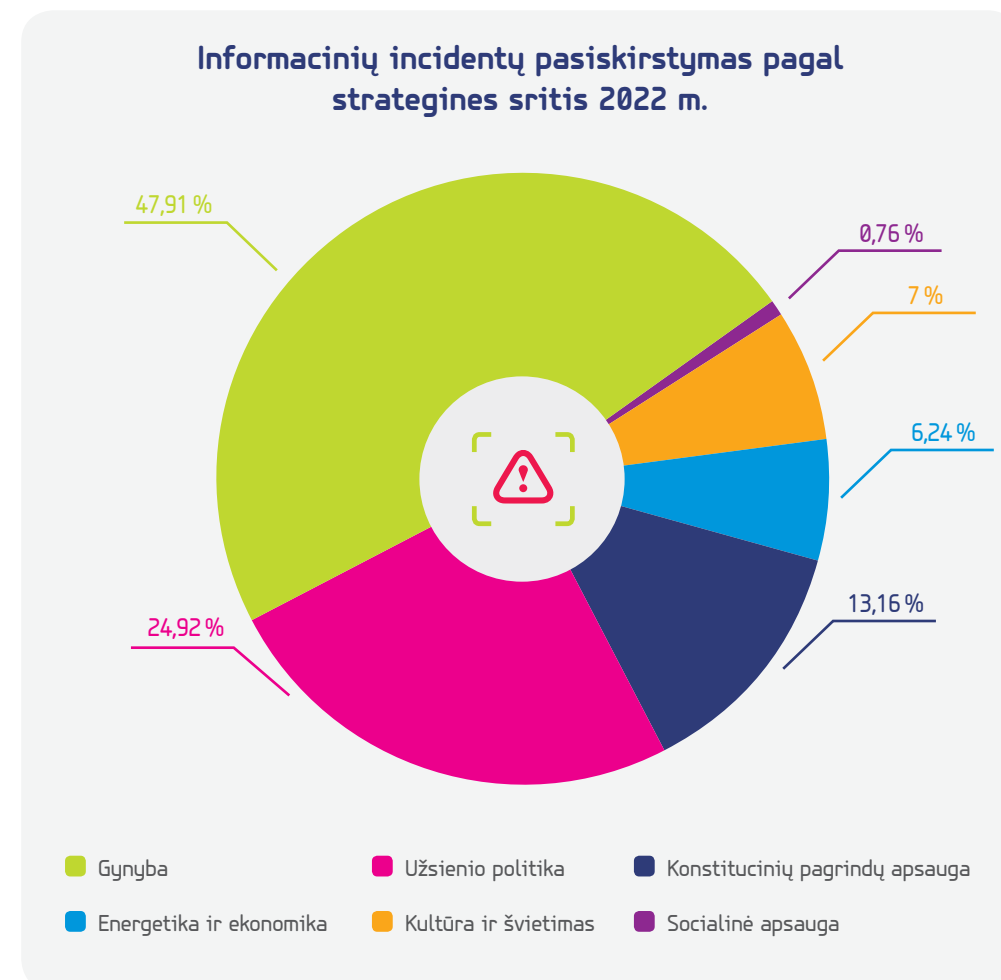
3 Informacinių incidentų skaičius pagal sritis

Vykdam 2022 m. informacinės aplinkos vertinimą, LK SKD stebėseną buvo orientuota į Lietuvai svarbias sritis: (1) gynybos, (2) užsienio politikos, (3) ekonomikos ir energetikos, (4) konstitucinių pagrindų apsaugos, (5) kultūros ir švietimo bei (6) socialinės apsaugos.

2022 m. priešiška veikla informacinėje aplinkoje pagal strategiškai svarbias Lietuvai sritis pasiskirstė taip: gynyba – 47,91 proc., užsienio politika – 24,92 proc., konstitucinių pagrindų apsaugos – 13,16 proc., ekonomikos ir energetikos – 6,24 proc., kultūros ir švietimo – 7 proc., socialinės apsaugos – 0,76 proc.

3 pav. >

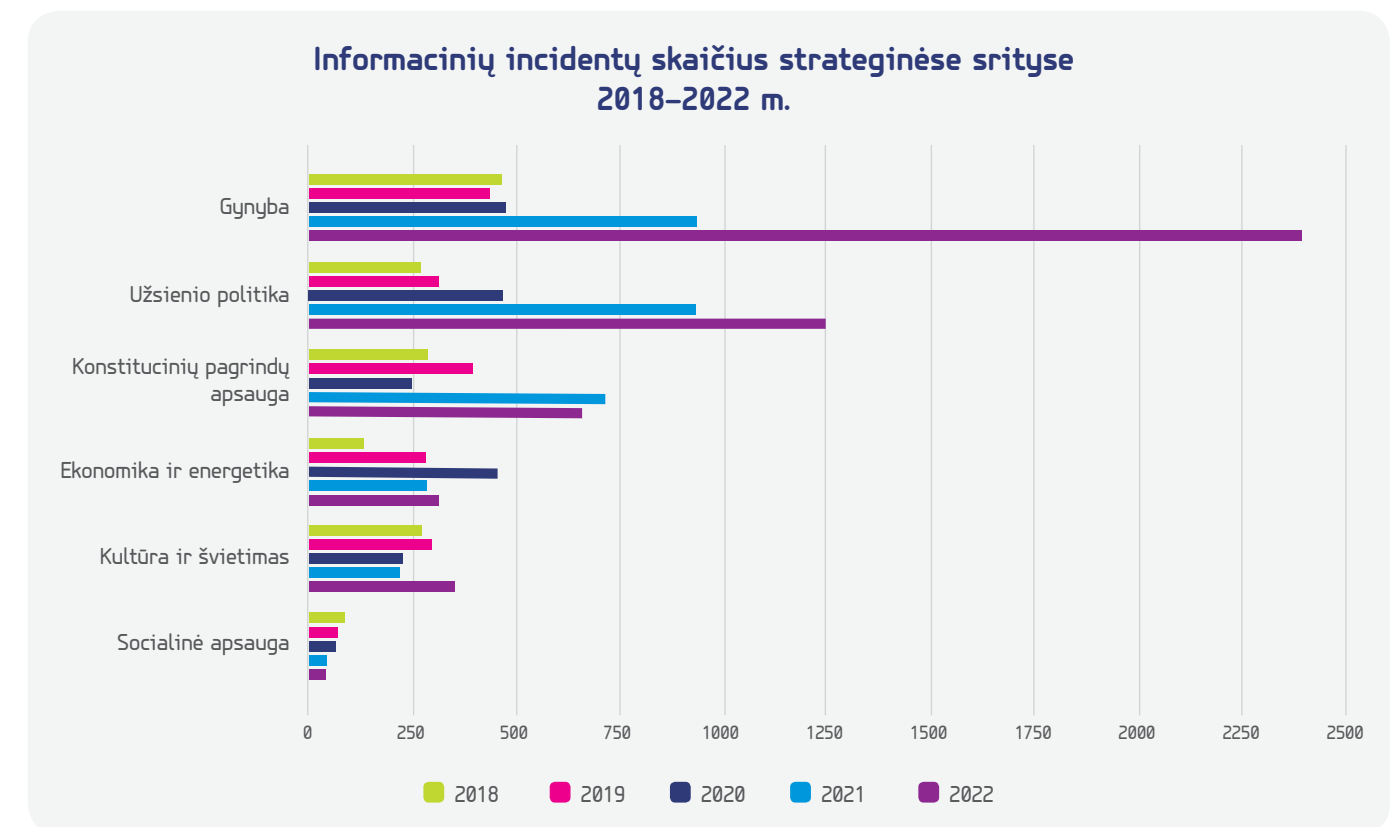
Informacinių incidentų pasiskirstymas pagal strategines sritis 2022 m. (šaltinis — LK SKD)



2022 m. fiksuota daugiausia unikalių informacinių atvejų sausio, gegužės, birželio, liepos, rugpjūčio, spalio mėn. Gynybos temų eskalacija 2022 m. išaugo beveik dvigubai: 2021 m. fiksuoti 26,42 proc. visų unikalių atvejų, o 2022 m. – 47,91 proc. Tai sutapo su reikšmingais užsienio ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti neigiamam šalies įvaizdžiui Vakaruose kurti ir Lietuvos visuomenės auditorijų tarpusavio susipriešinimui skatinti.

4 pav.

Informacinių incidentų skaičius strateginėse srityse 2017–2022 m. (šaltinis – LK SKD)



Dažniausi priešiški naratyvai 2022 m.

- 01 NATO yra agresyvus, puolantis karinis blokas
- 02 Lietuva yra nedemokratinė valstybė
- 03 Lietuva yra agresyvi valstybė
- 04 NATO savo veiksmais provokuoja Rusiją ir Baltarusiją
- 05 Lietuva yra socialiai, ekonomiškai ir politiškai žlugusi valstybė
- 06 NATO yra grėsmė Lietuvos nacionaliniam saugumui ir suverenitetui
- 07 Lietuva yra nereikšminga valstybė
- 08 NATO / Lietuva kišasi į kitų valstybių reikalus
- 09 Lietuvoje yra perrašomi ir klastojami istoriniai faktai
- 10 Lietuvos, ES energetiniai tikslai yra nepagrįsti

5 pav.

Dažniausi priešiški naratyvai 2022 m. (šaltinis — LK SKD)

4 Informacinių incidentų naratyvai

Gynybos srities naratyvai 2022 m. daugiausia buvo skirti dezinformacijai apie NATO ir Rusijos santykius skleisti. 2021 m. pradėjęs agresyvėti Rusijos propagandinis tonas apie NATO kaip provokatorę ir neva blogėjančios pasaulio saugumo situacijos kaltininkę netilo ir 2022 m. tiesiogiai kaltinant JAV ir NATO dėl karo Ukrainoje.

- > **Lietuvos gynybos ir saugumo politika** priešiškoje žiniasklaidoje 2022 m. sulaukė Kremliaus propagandos dėmesio dėl Lietuvos karinių pajėgumų stiprinimo, ginklų, technikos įsigijimo. Būta pranešimų, esą, užbaigus karą Ukrainoje, bus pradėtas JAV, NATO karas su Rusija Baltijos šalyse ir Lenkijoje.
- > **Branduolinio grasinimo retorika** buvo naudojama kaip stipriausias komunikacinis argumentas dialoge su Vakarais, siekiant palaužti JAV, NATO, ES lyderių vienybę dėl politinės ir karinės paramos Ukrainai.
- > **Užsienio politikos** temos 2022 m. sulaukė didelio Rusijos ir Baltarusijos kontroliuojamos žiniasklaidos susidomėjimo. Dėl užsienio politikos Lietuvą siekia pavaizduoti kaip nedemokratinę, agresyvią ir rusofobišką valstybę, vykdančią antirusišką politiką ir provokuojančią diplomatinį konfliktą tarp Rusijos ir Vakarų. Teigta, kad Lietuvos parama Ukrainai yra veiksmai, provokuojantys Rusiją. Siekta įtvirtinti nuostatą, kad Lietuva kišasi į Baltarusijos vidaus reikalus ir nori joje surengti perversmą.
- > **Socialinė visuomenės gerovė** priešinta su skiriamu per dideliu dėmesiu gynybai ir saugumui.
- > **2022 m. vykdytas didelis informacinis spaudimas** ir prieš ES dėl sankcijų Rusijai. Tokio didelio dezinformacijos ir manipuliacijos srauto nefiksuota nuo 2017 m. Aktyviai išnaudotas ES energetinės nepriklausomybės siekis nuo Rusijos, vykdytas informacinis spaudimas tiek Baltijos šalių, tiek ir ES gyventojams, siekiant įbauginti dėl ES kilusios energetikos krizės padarinių.
- > **Konstitucinių pagrindų apsaugos, socialinės apsaugos** sritys 2022 m. patyrė mažesnį informacinį spaudimą nei 2021 m. Dėl Baltarusijos režimo pradėtos hibridinės atakos Lietuvos ir Baltarusijos pasienyje dezinformacija konstitucinių pagrindų apsaugos temomis buvo itin išaugusi, tačiau 2022 m. neteisėta migracija, nors ir buvo vykdoma, tačiau nesukėlė reikšmingų pokyčių informacinėje aplinkoje.
- > **Informacinis spaudimas** Lietuvai skyrėsi nuo kitų NATO ir ES šalių dėl tik Lietuvai skirtos neigiamos informacijos. 2022 m. menkinta Lietuvos narystės Aljanse reikšmė, visuomenė buvo gąsdinama karu Baltijos šalyse, kurio metu NATO, esą, negins Lietuvos ir nevykdys įsipareigojimų.
- > **Menkintas ir Lietuvos kaip suverenios valstybės statusas.** Pabrėžta, kad Lietuva tėra nereikšminga valstybė tarptautinėje politinėje arenoje, priklausoma nuo JAV, NATO ir ES politinių bei ekonominių sprendimų, yra šalių lyderių vasalė, marionetė.
- > **2022 m. siekta įtvirtinti negatyvų požiūrį** į Lietuvos pagalbą karo pabėgėliams. Pabrėžta, kad Lietuva pabėgėlius iš Ukrainos išnaudoja tik savo interesams, siekia didesnės finansinės naudos iš ES, o mūsų šalies pagalba ukrainiečiams nėra nuoširdi.
- > **Dėl Lietuvos politinės ir karinės paramos Ukrainai** Lietuva kaltinta skatinanti karinius veiksmus Ukrainoje.

Informaciniu spaudimu siekta:

- ⚠ diskredituoti NATO kaip vieningą ir patikimą organizaciją;
- ⚠ silpninti Lietuvos gyventojų pasitikėjimą Lietuvos naryste Aljanse;
- ⚠ šmeižti Lietuvos vykdomą gynybos politiką Baltijos valstybių ir užsienio informacinėje aplinkoje;
- ⚠ menkinti Lietuvos kariuomenės įvaizdį, pajėgumus, gebėjimą pasipriešinti agresoriui;
- ⚠ diskredituoti Lietuvos užsienio politiką šalies viduje;
- ⚠ kurti Lietuvos kaip agresyvios ir rusofobiškos valstybės įvaizdį;
- ⚠ mažinti Lietuvos visuomenės paramą Ukrainai, Baltarusijos opozicijai, Taivanui;
- ⚠ diskredituoti valstybės institucijas;
- ⚠ kurti Lietuvos kaip nedemokratinės, politiškai žlugusios valstybės įvaizdį Lietuvos ir užsienio auditorijoms;
- ⚠ kurti Lietuvos kaip ekonomiškai ir energetiškai žlugusios valstybės įvaizdį Baltijos valstybių ir užsienio auditorijoms;
- ⚠ diskredituoti Lietuvos priimamus sprendimus dėl energetinės nepriklausomybės nuo Rusijos ir Baltarusijos;
- ⚠ kelti nepasitikėjimą valstybe dėl sprendimų socialinės gerovės klausimais.

5 Rezonansinės informacinės operacijos

2022 m. prieš Lietuvą ir valstybės institucijas įvykdyta mažiau priešiškų informacinių operacijų nei 2021 m. Mažesnį informacinių operacijų ir kibernetinių atakų prieš Lietuvos institucijas atvejų skaičių nulėmė Rusijos kibernetinių išpuolių prieš Ukrainos valstybines institucijas gausa. Baltijos šalims 2022 m. skirta daug mažiau dėmesio.

Išvados

Lietuvos informacinė aplinka yra gana saugi nuo Rusijos transliuojamos propagandos. Tačiau, nors mūsų žiniasklaida yra kritiškai mąstanti, vis tik pasitaiko pavienių priešiškų teiginių retransliavimo. Sistemingos ir sėkmingos Rusijos žiniasklaidos veiklos atvejų Lietuvoje nėra fiksuojama, išskyrus pavienius asmenis, kurie socialiniuose tinkluose dalijasi Rusijos skleidžiama dezinformacija. Tokie asmenys visuomenėje yra žinomi ir diskreditavę savo autoritetą.

Rusijos informacinėje aplinkoje, Kremliaus kontroliuojamuose žiniasklaidos kanaluose platinami Lietuvos pranešimams prieštaraujantys teiginiai, išvedžiojimai, manipuliacijos, dezinformacija ir kt. Rusijos informacinei erdvei kontroliuoti ir (ar) daryti didelę įtaką Lietuva neturi išvystytų pajėgumų ir resursų.

Pažymėtina, kad nuo toksiškos Rusijos ir Baltarusijos informacinės aplinkos Lietuvos visuomenė yra iš dalies atribota, todėl įtaka Lietuvai labiau matoma išorinėje informacinėje aplinkoje, ypač Rusijos ir Baltarusijos, o ne vidinėje – Lietuvos.

Rusijos karas prieš Ukrainą 2022 m. nulėmė spartesnį Lietuvos atsiribojimą nuo Rusijos informacinės erdvės. Lietuvoje uždraustas rusiškų, baltarusiškų kanalų retransliavimas, sistemingai kurtas Lietuvos institucijų požiūris į priešišką informacinę veiklą ir daromi žingsniai jai užkardyti, vykdytos pilietinės iniciatyvos ir išreikštas žiniasklaidos noras bendradarbiauti su Lietuvos kariuomene.

Rekomendacijos

Lietuvoje 2022 m. atsakingos institucijos toliau kėlė gyventojų medijų ir informacinio raštingumo lygį (MIR). Lietuvos piliečių sąmoningumo ir kritinio medijų turinio vertinimo įgūdžių bei kompetencijos ugdymas turi ir toliau likti pagrindinis Lietuvos informacinį atgrasymą užtikrinantis veiksnys.

Valstybinės ir socialinės žiniasklaidos priemonės turi siekti sumažinti Rusijos, Baltarusijos ir Kinijos valstybių kontroliuojamos žiniasklaidos manipuliavimo poveikį. Jeigu informacinio poveikio veiklos tikslas yra griauti pasitikėjimą institucijomis, kurstyti nesantaiką, kelti chaosą ir skatinti susiskaldymą visuomenėje, tai valstybė turi stiprinti savo bendravimo su visuomene priemones, didinti medijų raštingumą ir ugdyti kritinį mąstymą⁰².

Rekomendacijos visuomenei

LK SKD patarimai, kaip geriau atpažinti informacinius incidentus ir (ar) klaidinančią informaciją:

- ✓ Naudojantis informacija, reikėtų vadovautis sveiku protu ir įvertinti informacijos turinį. Būkite kritiški.
- ✓ Visuomet klauskite savęs: kas, kur, kodėl, kam, ką nori pasakyti, ar tai tikrai tiesa?
- ✓ Atsirinkite konkrečius informacijos šaltinius iš milijardų galimų, turinčius pridėtinę vertę ir teikiančius patikimą informaciją.
- ✓ Patikima informacija gali būti laikoma ta, už kurią laiduoja valstybės institucijos ir kurią skelbia patikimas, gerą reputaciją turintis šaltinis.
- ✓ Domėkitės pasirinktų informacijos kanalų veikla, akcininkais, žurnalistais.
- ✓ Patikrinkite informaciją bent keliuose kituose šaltiniuose.
- ✓ Pasirodžius neįprastai informacijai patikimuose kanaluose, galima įtarti, kad buvo įvykdyta hibridinė ataka ir neteisėtai paskelbta klaidinanti informacija, todėl rekomenduotina tuo pačiu metu naudoti bent du tris patikimus šaltinius.
- ✓ Įtarus, kad informacija galimai netiksli ar klaidinanti, rekomenduotina apie tai informuoti kanalo valdytoją.
- ✓ Neplatinkite nepatikimos, nepatvirtintos, klaidinančios informacijos socialiniuose tinkluose, artimųjų, draugų rate.
- ✓ Kiekvienas iš mūsų esame atsakingi už platinamą informaciją, todėl būkime atidūs ir netapkime priešiškos informacinės veiklos įrankiu.





Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
2023-05-31. Užsakymas Nr. GL-268

Dizaineris [Andrej Garbar](#)
Kalbos redaktorė [Inga Šorienė](#)
Naudotos iliustracijos iš [Freepik.com](https://www.freepik.com) grafinio archyvo

Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
[Vaizdinės informacijos skyrius](#), Totorių g. 25, LT-01121 Vilnius
Leidinio bibliografinė informacija pateikiama
[Lietuvos nacionalinės Martyno Mažvydo bibliotekos](#)

Nacionalinės bibliografijos duomenų banke (NBDB).

ISSN 2783-7017

© Lietuvos Respublikos krašto apsaugos ministerija
Atgaminti leidžiama nurodžius šaltinį



**NACIONALINĖ
KIBERNETINIO
SAUGUMO BŪKLĖS
ATASKAITA**

2022