2023–2030 m. plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos
priedas

2023–2030 METŲ PLĖTROS PROGRAMOS VALDYTOJOS LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJOS NACIONALINĖS KIBERNETINIO SAUGUMO PLĖTROS PROGRAMOS PAGRINDIMAS

PLĖTROS PROGRAMOS PASKIRTIS

Nacionalinio pažangos plano (toliau – NPP) pažangos uždavinys, kodas ir pavadinimas 10.5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“
Problema – dėl pasikeitusių kibernetinių grėsmių pobūdžio ir augančio jų masto mažėjantis šalies kibernetinis atsparumas. Paslaugų skaitmeninimas, naujų technologijų pritaikymas ir visuomenės narių įtraukimas į skaitmeninę erdvę vyksta sparčiau nei įvertinamos rizikos ir parenkamos tinkamos jų mažinimo priemonės ir būdai. Šis atotrūkis sudaro palankias sąlygas esamas spragas išnaudoti elektroniniams nusikaltimams vykdyti. Kibernetinių incidentų skaičius ir mastas 2016–2020 m. buvo linkęs didėti, nuo 2021 m. išlieka panašus (2016 m. užfiksuoti 489 didelės ir vidutinės reikšmės incidentai, 2017 m. – 536 didelės ir vidutinės reikšmės incidentai, 2019 m. – 3 241 incidentas, 2020 m. – 4 330 incidentų, 2021 m. – 4 088 incidentai, 2022 m. – 4 080 incidentų), tačiau su kiekvienais metais keičiasi grėsmių pobūdis, atakų vykdymo būdas ir sudėtingumas[1]. 2022 m. Nacionalinio kibernetinio saugumo būklės ataskaitoje nurodoma, kad daugiausia kibernetinių incidentų užfiksuota valstybės ir savivaldybių, saugumo ir gynybos bei verslo įmonių infrastruktūrose. ENISA ataskaitoje nurodoma, kad 2021–2022 m. kibernetinės atakos buvo nukreiptos į viešojo sektoriaus institucijas (24 proc.), skaitmeninių paslaugų teikėjus (13 proc.), visuomenę (12 proc.), paslaugas (12 proc.), finansų sektorių (7 proc.), sveikatos apsaugos sektorių (7 proc.), transporto sektorių (4 proc.), energetikos sektorių (4 proc.), švietimo sektorių (2 proc.) [2]. Kibernetinių atakų gausa ir pavojingumas tiek organizacijose, tiek ekonominės veiklos sektoriuose reikalauja naujų kibernetinių incidentų ir informacijos saugos mechanizmų ir esamų pajėgumų sustiprinimo, siekiant sukurti saugią aplinką informacinėms ir ryšių technologijoms (toliau – IRT) veikti, saugaus veikimo sąlygoms nustatyti ir jų nuolatinei stebėsenai vykdyti. Kibernetinio incidento pasekmės sukelia neproporcingai daug žalos ir daro neigiamą įtaką organizacijų reputacijai (klientų pasitikėjimo ar įvaizdžio praradimas, nepasitikėjimas skaitmenine erdve), paslaugų skaitmenizavimui (nepasiekiamos informacinės sistemos, sugadinti duomenų rinkiniai), išlaidoms (remontas, naujų priemonių įsigijimas, prarastas našumas, inovacijos lėšų praradimas jas skiriant veiklai atkurti po kibernetinio incidento), fiziniam saugumui

[1] Pagal Nacionalinis kibernetinio saugumo centro prie Krašto apsaugos ministerijos ir Krašto apsaugos ministerijos rengtas Nacionalinio kibernetinio saugumo būklės ataskaitas 2020, 2021, 2022 m.
[2] ENISA. *Threat Landscape 2022.*

(klientų, pacientų, darbuotojų fizinis sužalojimas), socialinei tvarkai (kritinės infrastruktūros – energetikos, transporto, finansų, sveikatos apsaugos ir kt. – sutrikdymas)[3].

Europos Sąjungos (toliau – ES) mastu 2021 m. atlikta ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdytojų ir skaitmeninių paslaugų teikėjų apklausa[4] parodė, kad minimali kibernetinio incidento žala prasideda nuo 30 tūkst. Eur ir gali siekti 2 mln. Eur pavojingo incidento atveju. Tam tikrais atvejais socialinė ir ekonominė kibernetinio incidento žala gali būti neproporcingai didelė – daug didesnė nei poveikis techniniu aspektu, pvz., paciento mirtis gydymo įstaigoje dėl apribotos prieigos prie kenkimo programinės įrangos užšifruotų duomenų[5].

Lietuvos visuomenės kibernetinio saugumo žinios ir taikomieji gebėjimai taip pat nėra pakankami: 73 proc. 16–74 metų amžiaus asmenų naudojosi valstybės institucijų ar viešųjų įstaigų interneto svetainėmis, 59 proc. siuntėsi blankus, kopijavo ar perkėlė rinkmenas į įrenginius, aplankus, tačiau tik 36 proc. prieš teikdami asmens informaciją perskaitė privatumo taisykles, 20 proc. patikrino, ar interneto svetainė, kurioje reikia pateikti asmens informaciją, yra saugi, 3 proc. abejodami dėl interneto saugumo susilaikė nuo naudojimosi viešąja belaidžio interneto prieiga (angl. *WiFi*), 93 proc. teigė nesusidūrę su interneto saugumo problemomis[6]. Didelis piliečių pasitikėjimas skaitmenine erdve ir tuo pačiu metu augantys kibernetinių incidentų skaičiai bei per nusikalstamas veikas patiriamų nuostolių dydis rodo prieštarą tarp visuomenės lūkesčių ir gebėjimų įvertinti situaciją.

1. Esamas kibernetinio saugumo modelis netinkamas augančiai kibernetinio saugumo sričiai:

1.1. Plečiantis kibernetinio saugumo taikymo sričiai trūksta kibernetinio saugumo politikos įgyvendinimo procese dalyvaujančių suinteresuotųjų subjektų.

Europos Parlamentas ir Taryba 2022 m. pabaigoje priėmė direktyvą (ES) 2022/2555[7], kurios įgyvendinimas reikalauja iš esmės peržiūrėti nacionalinę kibernetinio saugumo politikos formavimo ir įgyvendinimo sistemą, į kibernetinio saugumo valdymą ir užtikrinimą įtraukiant daugiau institucijų. Šiuo metu Kibernetinio saugumo įstatymu nustatyta kibernetinio saugumo politikos formavimo ir įgyvendinimo sistema, paremta penkioms institucijoms paskirstytomis funkcijomis, nėra pakankamai lanksti į Direktyvos (ES) 2022/2555 taikymo sritį patenkantiems subjektams ir sektoriams vertinti, taikytinoms priemonėms ir taisyklėms nustatyti, griežtesnei kontrolei vykdyti bei griežtesnėms sankcijoms taikyti.

Kibernetinio saugumo politikos formavimas taip pat neapėmė kibernetinio saugumo reikalavimų taikymo atvirojo interneto viešojo pagrindo prieinamumo, vientisumo ir konfidencialumo (įskaitant povandeninius ryšių kabelius), pažangių technologijų kūrimo ir integravimo, mokslinių tyrimų ir technologinės plėtros iniciatyvų, gerosios kibernetinės higienos praktikos ir kontrolės gairių, skirtų piliečiams, aktyvios kibernetinės apsaugos srityse. Direktyva (ES) 2022/2555 rodo kibernetinio saugumo taikymo srities plėtimąsi ir skverbimąsi į įvairias veiklos sritis. Ši tendencija reikalauja iš naujo įvertinti esamą kibernetinio saugumo politikos formavimo ir įgyvendinimo sistemą, t. y. įvairių institucijų bei atitinkamų suinteresuotųjų subjektų vaidmenis ir

[3] ENISA. *Threat Landscape 2022*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[4] ENISA. *NIS Investments*, 2022, https://www.enisa.europa.eu/publications/nis-investments-2022.

[5] OECD. *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, 2022, https://doi.org/10.1787/a69df866-en.

[6] Valstybės duomenų agentūra. Oficialiosios statistikos portalas. *Asmenys, naudojęsi valstybės institucijų ar viešųjų įstaigų interneto svetainėmis. Asmenys, kurie atliko išvardytus veiksmus, susijusius su prieiga prie asmeninės informacijos internete. Asmenys, kuriuos abejonės dėl interneto saugumo sulaikė nuo tam tikrų veiksmų internete. Asmenys, susidūrę su interneto saugumo problemomis*, https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/.

[7] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva), https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32022L2555&from=EN.

pareigas įgyvendinant, bendradarbiaujant ir koordinuojant veiklą nacionaliniu lygiu, kartu įvertinant valstybės informacinių išteklių valdymo ir kibernetinio saugumo valdymo sąsajas.

1.2. Nesukurti kibernetinio saugumo reikalavimų atnaujinimo metodai.

Organizaciniai ir techniniai kibernetinio saugumo reikalavimai (toliau – OTR) yra nelankstūs ir neapima naujų bei vis labiau įsigalinčių technologijų reikalavimų kibernetiniam saugumui. OTR stebėsenos ir analizės modeliai, metodai, kryptys, kurie galėtų būti realizuoti naudojant IRT, nepakankamai išvystyti nacionaliniu lygiu.

Aukštas kibernetinio saugumo reikalavimų užtikrinimo lygis, atsižvelgiant į kintančias kibernetines grėsmes, nebus pasiektas neperžiūrėjus ir neatnaujinus OTR valstybės informaciniams ištekliams, valstybės valdomiems elektroninių ryšių tinklams nustatančių teisės aktų. Reikia tobulinti ir atskirus teisės aktus, pagal kuriuos vyksta kibernetinio saugumo rizikų vertinimas, taip pat peržiūrėti ir atnaujinti rekomendacijas mažoms ir vidutinėms įmonėms (toliau – MVĮ).

Tikimasi, kad kibernetinio saugumo reglamentavimo peržiūra leis atnaujinti kibernetinio saugumo valdymą bei OTR formavimo sistemą ir sudarys prielaidas didesniam kibernetinio saugumo integravimui į kasdienę organizacijų veiklą.

1.3. Skirtingai taikomos kibernetinio atsparumo priemonės viešajame sektoriuje.

ES mastu 2021 m. atlikta 1080 YSII valdytojų ir skaitmeninių paslaugų teikėjų 27 ES šalyse apklausa[8] parodė, kad informacinių technologijų (toliau – IT) investicijos kasmet vidutiniškai sudarė 10 mln. Eur, informacijos saugos investicijos – 0,6 mln. Eur, t. y. informacijos saugos investicijos sudaro 6,7 proc. visų IT investicijų. Pagal šią apklausą Lietuvos IT investicijos sudarė 3 mln. Eur (tiek pat kiek Estijos ir Slovėnijos, mažesnės investicijos buvo tik Latvijoje, Maltoje ir Kipre), informacijos saugos investicijos sudarė 0,2 mln. Eur (mažesnės investicijos buvo tik Latvijoje, Estijoje, Slovėnijoje, Maltoje ir Kipre). Pripažįstama, kad kibernetinio saugumo iniciatyvos negali palaikyti aukšto skaitmeninės transformacijos tempo, šioms iniciatyvoms skiriami biudžetai nedidėja taip greitai kaip kibernetinio saugumo rizikos, su kuriomis susiduriama tiesiogiai. Skaitmenizacijos plėtros ir kibernetinio saugumo stiprinimo šuolius, kai neįprastai daug dėmesio ir resursų skiriama tikslams kiek įmanoma greičiau pasiekti vienu ar kitu technologiniu aspektu, galima matyti krizių laikotarpiu, pvz., COVID-19 pandemijos metu pagrindiniais kibernetinio saugumo prioritetais organizacijos laikė saugias skaitmeninės transformacijos iniciatyvas (94,5 proc.), naudojimąsi kibernetinio saugumo paslaugomis (angl. *security-as-aservice*) (89 proc.), nulinio pasitikėjimo architektūros (angl. *zero trust architecture*) įgyvendinimą (89 proc.), saugų bendradarbiavimą (77,5 proc.), daugiafaktorį identifikavimą (67,5 proc.), nuotolinį prisijungimą šifruotu ryšiu (56,5 proc.)[9].

Vertinant valstybės institucijų atitiktį OTR, nustatyta, kad juos kibernetinio saugumo subjektai (toliau – KSS) įgyvendina skirtingai, dažnai juos atitinka arba beveik atitinka tik *de jure*. Jei organizacijos ir turi formaliai apibrėžtus kibernetinio saugumo procesus, gaires, tačiau kibernetinio saugumo užtikrinimas dažnai jų vertinamas kaip biurokratinė našta[10]. Kelerių metų vertinimas parodė, kad valstybės informacinių išteklių ir YSII valdytojų ir tvarkytojų OTR įgyvendinimo lygis nesikeičia ir vis dar yra nepakankamas[11]. Įgyvendinant OTR *de facto* tik iš dalies, neužtikrinamas pakankamas kibernetinio saugumo lygis.

[8] ENISA. *NIS Investments*, 2022.
[9] STATISTA. *Post-pandemic cybersecurity priorities worldwide 2020*, 2022, https://www.statista.com/statistics/1228924/post-pandemic-cybersecurity-priorities/.
[10] NKSC. *Nacionalinio kibernetinio saugumo būklės ataskaita*, 2019, https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf.
[11] KAM. *Nacionalinė kibernetinio saugumo ataskaita 2021*, 2022, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf.

Stebint organizacijų Didžiojoje Britanijoje elgesio ir požiūrio pasikeitimus, nustatyta tendencija, kad organizacijos kibernetinį saugumą suvokia kaip labiau reaktyvų, nei proaktyvų veikimą, o proaktyvų veikimą skatina tik patirtas kibernetinis incidentas ar paslaugų teikimo sutartyse nurodytas reikalavimas laikytis tarptautinių ar visuotinai pripažintų standartų[12]. Vis dėlto sertifikavimosi pagal visuotinai pripažintus standartus negalima laikyti baigtiniu organizacijos kibernetinio saugumo užtikrinimo etapu, kibernetinio saugumo valdymas yra nuolatinis procesas.

Nustatyti kibernetinės brandos lygiai sudarys galimybę pačioms organizacijoms nustatyti tobulinimo kryptis.

Stiprinant IRT atsparumą, prioritetą būtina teikti valstybės institucijoms ir įstaigoms, kurių veikla susijusi su kritiškai svarbių paslaugų teikimu, ar teikiančioms paslaugas kitoms valstybės institucijoms ir įstaigoms. Saugiojo valstybinio duomenų perdavimo tinklo (toliau – ST) paslaugos skirtos institucijoms, kurios valdo ar tvarko informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti. Atsižvelgiant į ST esančių institucijų ir jų informacinių išteklių ypatingą svarbą ir didelius informacijos kiekius, ST tampa vienu iš pirmųjų ir dažnu kibernetinių atakų taikiniu. Šiuo metu ST naudojamos kolektyvinės apsaugos kibernetinio saugumo priemonės fiksuoja daugiau nei 180 tūkst. įvairiausių saugos įvykių per parą, o dažniausias kibernetinės atakos tipas – paskirstyta paslaugos trikdymo ataka (angl. *DDoS*). Kibernetinės atakos dažniausiai yra kompleksinės, sudėtingos ir, nors nukreipiamos į konkretų informacinį išteklių, kartu sutrikdoma ir kitų SVDPT esančių institucijų veikla, sukeliama žala jų informaciniams ištekliams. Esama ST informacinių išteklių sąveikos ir kibernetinės saugos architektūra neleidžia apriboti kenkimo veiklos masto bei taikyti tikslinių kibernetinių saugumo priemonių, nes esami ST infrastruktūros komponentai nėra visiškai sugrupuoti, apribota jų prieiga prie viešųjų elektroninių ryšių tinklų.

Tikimasi, kad įgyvendinus centralizuotus sprendimus bus padidintas ne tik ST atsparumas kibernetinėms atakoms, bet ir bus užtikrintas kritinių valstybės informacinių išteklių pasiekiamumas, net ir daliai jų esant nepasiekiamiems.

Kibernetinio atsparumo priemonių kaip organizacinių struktūrų nustatymas, vienodų standartų diegimas viešojo sektoriaus įstaigose padidintų viešojo sektoriaus įstaigų kibernetinį atsparumą.

Šiuo metu nėra nustatytos saugumo operacijų centrų (angl. *Security Operation Center* (SOC)), kompiuterinių incidentų tyrimo (reagavimo) tarnybų (angl. *Computer Emergency Response Team* (CERT)), reagavimo į kompiuterinius saugumo incidentus tarnybų (angl. *Computer Security Incident Response Team* (CSIRT)) kūrimo ir vystymosi kryptys, nuoseklūs jų bendadarbiavimo mechanizmai. Lietuvoje SOC, CSIRT, CERT tinklas buvo vystomas daugiau reaktyviai, remiantis organizacijų iniciatyva, nei planingai ir sistemingai. Lietuvoje šiuo metu veikia akademinio sektoriaus specifikai pritaikyta kibernetinio saugumo incidentų tyrimų tarnyba LITNET-CERT, nacionalinė NKSC-CERT, privačiame sektoriuje veikia BITE-SOC, TEO-CERT, NRD-CIRT, IGNITIS-CERT[13]. SOC, CERT ar CSIRT įveiklinimo pagrindinis pokytis – trumpėja incidentų valdymo bei tyrimo laikas. Saugumo ir incidentų valdymo srities veiklos ir funkcijų struktūrizavimo per SOC, CSIRT ir CERT efektyvumas pasireiškia gebėjimu struktūrizuoti informaciją, kaupti ir sisteminti specifines kibernetinio saugumo žinias, atitinkamai tobulinti procesus ir technologijas, nuolatine stebėsena, koncentracija į saugumo klausimus, sklandesnėmis informacijos mainų procedūromis su kitomis institucijomis ir organizacijomis bei sukaupta kompetencija.

[12] GOV.UK. *Cyber security longitudinal study – wave two*, 2022, https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-two-results/cyber-security-longitudinal-study-wave-two.

[13] ENISA. *CSIRTs by Country – Interactive Map*, 2022, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#constituency=Research%20%26%20Education.

Tikimasi, kad nustatyti standartizuoti mechanizmai ir organizacinės struktūros sudarys galimybę organizacijoms patobulinti saugumo ir incidentų valdymą.

1.4. Kibernetinio saugumo, atsparumo ir grėsmės lygio vertinimui trūksta kibernetinio saugumo stebėsenos duomenų.

Pagrindinis įrankis, skirtas KSS keistis informacija apie galimus ir įvykusius kibernetinius incidentus bei kita su kibernetinio saugumo užtikrinimu susijusia informacija tarpusavyje ir su NKSC, yra NKSC valdomas Kibernetinio saugumo informacinis tinklas (toliau – KSIT). Vis dėlto KSS KSIT nesinaudoja dėl įvairių priežasčių[14]. Priežasčių, neužtikrinančių institucijų optimalaus bendradarbiavimo, identifikavimas ir šalinimas, iš naujo įvertinant KSS organizavimosi galimybes per KSIT, sudarytų sąlygas didinti informuotumą. Taip pat, atsižvelgiant į kintantį grėsmių pobūdį, jų dinamiką, naujas technologijas, trūksta papildomo vertinimo, ar esamos KSIT paslaugos yra pakankamos kibernetinėms grėsmėms mažinti ir ar yra pritaikytos prie pasikeitusių grėsmių. Naujų bendradarbiavimo formų ir platformų atsiradimas, į informacijos mainus įtraukiant daugiau suinteresuotų šalių, leistų efektyviau keistis informacija bei sudarytų sąlygas tolesniam bendradarbiavimui.

Pradedamos naudoti technologijos ne visada turi nustatytus ir joms taikomus kibernetinio saugumo reikalavimus, todėl ypač svarbu periodiškai atlikti ne tik IRT atitikties teisės aktams vertinimą bei sistemingą OTR įgyvendinimo stebėseną, bet ir kibernetinio saugumo rizikų vertinimą, leidžiantį nedelsiant identifikuoti realioje situacijoje kylančias grėsmes.

Šiuo metu valstybės informacinių išteklių ir YSII kibernetinio saugumo rizikų ir atitikties teisės aktams vertinimo rezultatai kaupiami NKSC, dalį duomenų suvedant į Informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą (toliau – ARSIS). Atsižvelgiant į ARSIS pajėgumus ir funkcionalumus bei kylantį poreikį kaupti išsamią informaciją apie IRT atitikties teisės aktams vertinimą, OTR įgyvendinimo stebėseną bei kibernetinio saugumo rizikų vertinimą, buvo nustatyta, kad ARSIS funkcionalumai nėra pakankami išsamiam IRT kibernetinio atsparumo vertinimui atlikti. Atsižvelgiant į nustatytus trūkumus, esama sistema be vystymo krypčių analizės nesudarys sąlygų vykdyti išsamią OTR įgyvendinimo stebėseną.

Tinkamų organizacinių ir techninių priemonių, kurios yra viena iš sąlygų norint palaikyti didelį apsikeitimo informacija greitį, parinkimas leistų užtikrinti operatyvesnį informacijos pateikimą sprendimus kibernetinio saugumo srityje priimantiems asmenims.

1.5. Nenuosekliai vykdomas valstybės institucijų personalo švietimas ir edukacija kibernetinio saugumo klausimais.

NKSC nuolat vykdo bazinius ir specialiuosius kibernetinio saugumo mokymus viešojo sektoriaus darbuotojams bei organizuoja kibernetines pratybas. 2021 m. šiuos mokymus išklausė virš 2 tūkst. viešojo sektoriaus darbuotojų iš daugiau kaip 20 įstaigų, buvo organizuoti ir specialūs kibernetinio saugumo mokymai[15]. Praktinis įgytų žinių patikrinimas, praktinių įgūdžių įtvirtinimas bei bendradarbiavimo gerinimas vykdomas prisijungiant prie kibernetinio saugumo pratybų, kurių rezultatai leidžia parinkti tolesnes mokymo bei procesų tobulinimo kryptis.

Lietuvoje kasmet vyksta nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas“, kurias organizuoja NKSC kartu su partneriais iš mokslo institucijų. Šios pratybos vykdomos remiantis mokymosi realiomis sąlygomis principu (angl. *train as you fight*), t. y. dalyviai pratyboms specialiai nesiruošia ir dalyvauja su tokiais pajėgumais, personalu ir procedūromis, kuriuos realiai turi. Tai leidžia organizacijai pamatyti tikrą savo kibernetinio saugumo būklę ir įsivertinti turimus gebėjimus reaguoti į įvairaus tipo kibernetinius incidentus[16]. 2020 m. šiose pratybose dalyvavo 760 asmenų iš 73 organizacijų, 2021 m.

[14] Valstybės kontrolė. *Valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas“*, 2022, https://www.valstybeskontrole.lt/LT/Product/24128/kibernetinio-saugumo-uztikrinimas.
[15] NKSC. *Darbuotojai išlieka silpniausia kibernetinio saugumo vieta*, 2021, https://www.nksc.lt/naujienos/darbuotojai_islieka_silpniausia_kibernetinio_saugu.html.
[16] NKSC. *Penktadaliu išaugo kibernetinio saugumo pratybų „Kibernetinis skydas 2021“ dalyvių skaičius,* 2021, https://www.nksc.lt/naujienos/penktadaliu_isaugo_kibernetinio_saugumo_pratybu_ki.html.

– 670 asmenų iš 92 organizacijų, 2022 m. – 116 organizacijų [17, 18, 19]. Didesnę dalyvių dalį sudaro valstybės informacinių išteklių arba YSII valdytojai arba tvarkytojai, taip pat dalyvauja sveikatos priežiūros įstaigos, energetikos bendrovės, finansų institucijos, universitetai ir kt. Pastebimas kasmet didėjantis poreikis prisijungti prie pratybų, plečiasi dalyvaujančių institucijų spektras. Vis dėlto 2021 m. pratybose dalyvavo tik 21,7 proc. visų valstybės informacinių išteklių arba YSII valdytojų arba tvarkytojų[20], o 2022 m. nebuvo pasiektas nacionalinėse kibernetinio saugumo pratybose dalyvaujančių YSII ir valstybės informacinių išteklių valdytojų rodiklis, todėl siektina didinti į įvairias kibernetinio saugumo pratybas įtraukiamų organizacijų skaičių.

Tikimasi, kad sudarytos sąlygos nuosekliam valstybės institucijų darbuotojų švietimui ir edukacijai padės organizacijoms didinti ir (ar) atnaujinti žinias kibernetinio saugumo srityje.

1.6. Trūksta kibernetinio saugumo specialistų.

Atskirų tyrimų, skirtų kibernetinio saugumo specialistų pakankamumui viešajame sektoriuje įvertinti, yra mažai, todėl remiamasi bendrų, tiek viešąjį, tiek privatų sektorius apimančių, tyrimų duomenimis. Tarptautinių tyrimų duomenys rodo kibernetinio saugumo specialistų ir įvairių jų kompetencijų trūkumą: trūksta apie 3 mln. kibernetinio saugumo profesionalų [21, 22, 23], net 95 proc. verslo organizacijų, kuriose dirba mažiau nei 100 darbuotojų, informacijos saugumo specialistų neturi. Šis trūkumas kritinis aviacijoje, valstybiniame sektoriuje, švietimo, draudimo ir transporto srityse. 2020 m. duomenimis, atlikus 1,5 mln. ES valstybėse veikiančių įmonių apklausą[24], iš kurių 83 proc. buvo mažos įmonės, 55 proc. įmonių trūko IT specialistų (Lietuva viršijo šį ES vidurkį su 59 proc. rodikliu). ENISA 2021 m. apklausos metu[25] YSII ir skaitmeninių paslaugų teikėjai nurodė, kad siekia įgyti kompetencijų ar jiems trūksta personalo tokiose srityse kaip: incidentų valdymas, grėsmių analizė, rizikos valdymas, paslaugų valdymas ir pan. Lietuvoje pastaruosius penkerius metus daugiau nei 50 proc. valstybės ir savivaldybių institucijų susiduria su IT specialistų trūkumu, 2021 m. 62 proc. įmonių turėjo neužimtas IT specialistų vietas[26].

KAM užsakymu Vilniaus universiteto ir Generolo Jono Žemaičio Lietuvos karo akademijos mokslininkų parengta studija ir atlikta įmonių vadovų ir žmogiškųjų išteklių skyrių vadovų apklausa[27] parodė, kad Lietuvoje taip pat didžioji dalis mažų įmonių (iki 10 darbuotojų) neturi vien tik už kibernetinį saugumą atsakingų specialistų, jų taip pat stokoja ir didesnės įmonės (pusė apklaustų įmonių). Apklausos metu nustatyta, kad per artimiausius 2–5 metus Lietuvoje didžiosios įmonės (virš 50 darbuotojų) ieškos 800 naujų kibernetinio saugumo specialistų.

---

[17] NKSC. *Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas 2021“ ataskaita visuomenei*, https://www.nksc.lt/doc/KS2021_pratybu_ataskaita.pdf.
[18] NKSC. *Darbuotojai išlieka silpniausia kibernetinio saugumo vieta,* 2021.
[19] NKSC. *Nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2022“ ataskaita*, 2022. https://www.nksc.lt/doc/KS2022_pratybu_ataskaita.pdf.
[20] NKSC. *Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas 2021“ ataskaita visuomenei*.
[21] ISACA. *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperation*, https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf.
[22] *(ISC)² Cybersecurity Workforce Study*, 2022. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.
[23] World Economic Forum. *The Global Risks Report 2022*.
[24] Eurostat. *ICT specialists - statistics on hard-to-fill vacancies in enterprises*, 2020, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises.
[25] ENISA. *NIS Investments*, 2022.
[26] Valstybės duomenų agentūra. Oficialiosios statistikos portalas. *Valstybės ir savivaldybių įstaigos, susiduriančios su IT specialistų trūkumu. Įmonės, turėjusios IT specialistų laisvų darbo vietų, kurias sunku buvo užpildyti*.
[27] Vilniaus universitetas ir Generolo Jono Žemaičio Lietuvos karo akademija. *Lietuvos kibernetinio saugumo kompetencijų žemėlapis (ataskaita)*, 2022, https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf.

Atsižvelgiant į tai, labai svarbu populiarinti kibernetinio saugumo specialisto profesiją, mažinti moterų atskirtį, anksti įtraukti jaunus žmones, aiškiai komunikuojant apie kibernetinio saugumo specialistų reikšmę ir perspektyvas, nes, nors kibernetinio saugumo sritis yra patraukli ir atrodo perspektyvi naujiems darbo rinkos dalyviams ar keičiantiems savo profilį, tačiau pastarieji ne visada supranta, kokios funkcijos turi būti atliekamos, arba, siekdami įsidarbinti, pervertina turimas žinias.

2. Nusikalstamų veikų elektroninėje erdvėje tyrimo pajėgumai neatitinka nusikalstamų veikų sudėtingumo.

Nusikaltimų elektroninėje erdvėje dinamika ir kompleksiškumas didėja. Identifikuojamos šios pagrindinės tendencijos: formuojasi nauja paslaugų rinka – nusikaltimas kaip paslauga (angl. *crime-as-a-service*), apimanti prieigų suteikimo, išpirkos reikalaujančių programų paslaugas, taip pat auga kibernetinių nusikaltėlių susidomėjimas debesijos technologijų spragomis, tiekimo grandinių atakomis, prieš industrines sistemas nukreiptomis atakomis[28, 29]. Be to, didėja ir iš nusikalstamos veiklos gautų finansų srautai. Prognozuojama, kad bendra kibernetinių nusikalstamų veikų keliama žala nuo 11,50 trilijono dolerių 2023 m. padidės iki 23,82 trilijono dolerių 2027 m.[30]. Nuolat tobulinami nusikalstamoms veikloms vykdyti naudojami įrankiai, kuriuos standartinėmis kibernetinio saugumo priemonėmis tampa vis sunkiau aptikti. Nusikaltimams elektroninėje erdvėje vykdyti išnaudojamos bet kokios palankios situacijos, pvz., COVID-19 pandemija, kurios metu nuotolinio darbo specifika sudarė palankesnes sąlygas išnaudoti organizacines ir technologines spragas bei socialinę inžineriją skverbiantis į organizacijų tinklus ar gauti naudą iš suklastotų internetinių parduotuvių ir apgaulingų investavimo galimybių; išnaudojamos naujų technologijų spragos, taip rasta mobiliesiems telefonams skirtos kenkimo programinės įrangos niša, įsigalėjo kriptovaliutomis grįstos nusikalstamos veikos, neteisėtais ir nusikalstamais būdais gauti finansai paverčiami kriptovaliuta. Dideles rizikas atneša ir naujosios technologijos – daiktų internetas (angl. *IoT*), dirbtinis intelektas. Situacija tampa dar sudėtingesnė, jei nusikalstama veika vykdoma už nacionalinės valstybės jurisdikcijos ribų ar nusikalstamas veikas vykdantys asmenys tarpusavyje bendradarbiauja. Pažymėtina ir tai, kad didelė dalis nusikaltimų elektroninėje erdvėje taip ir lieka neidentifikuoti arba apie juos nepranešama.

Vertinant Lietuvoje vykdomų nusikalstamų veikų elektroninėje erdvėje užkardymą, atskleidimą ir tyrimą nustatyta trūkumų: nesudarytos sąlygos rezultatyviai atlikti nusikaltimų elektroninėje erdvėje tyrimus, trūksta specializuotų pajėgumų nusikaltimams elektroninėje erdvėje tirti, neefektyvus informacinių technologijų tyrimams (apžiūroms) atlikti reikalingos specializuotos įrangos įsigijimo mechanizmas, fragmentuotas atsakingų padalinių aprūpinimas reikalinga įranga, ribotos finansinės ir organizacinės galimybės specializuotuose padaliniuose įdarbinti darbuotojus, turinčius techninės srities išsilavinimą ir (ar) gebėjimus[31]. Taip pat išryškėjo tendencija, jog esamos elektroninių nusikaltimų tyrimo pajėgos nėra pakankamos, nėra galimybių išlaikyti kompetentingų specialistų. Didesnė dalis šių trūkumų bus šalinama bei įvairių priemonių problematika ir poreikis analizuojamas Viešojo saugumo stiprinimo ir plėtros programoje.

2.1. Nevystoma elektroninių nusikaltimų tyrimo infrastruktūra.

[28] Europol, 2021. *Internet organised crime threat assessment 2021*.
[29] ENISA. *Threat Landscape 2022.*
[30] STATISTA. *Cybercrime Expected To Skyrocket in Coming Years*, 2022, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.
[31] Valstybės kontrolė. *Valstybinio audito ataskaita „Ar veiksingai kovojama su elektroniniais nusikaltimais“*, 2021, https://www.valstybeskontrole.lt/LT/Product/23926/ar-veiksmingai-kovojama-su-elektroniniais-nusikaltimais.

Elektroniniams nusikaltimams pasitelkiamos legitimios paslaugos, pasižyminčios stipriomis šifravimo galimybėmis, saugūs komunikacijos kanalai (VPN), naudojamos sudėtingos blokų grandinės (angl. *blockchain*) technologijos[32], todėl rekomenduojama tobulinti technines galimybes, ypač duomenų analizės įrankius, naudoti blokų grandinės technologijas.

Tirdama kibernetines atakas ir nusikaltimus elektroninėje erdvėje prieš valstybines institucijas bei YSII, taip pat atakas, kai kėsinamasi į asmens duomenis, Lietuvos policija turi paimti bei išsaugoti itin daug duomenų, kurie reikalauja operatyvios analizės. Sudėtingiausiuose tyrimuose ekspertų atsakymai dėl tyrimo krypties turi būti gauti nedelsiant, kad tyrėjai turėtų galimybę užkardyti nusikalstamas veikas, apsaugoti ir paimti perimtus (pavogtus) duomenis, mažinti galimą žalą ir grėsmes, nustatyti tikruosius įtariamųjų interneto protokolo (angl. *IP*) adresus ir surinkti kitus skaitmeninius įrodymus. Sparčiai didėjant kibernetinių atakų kompleksiškumui ir sudėtingumui reikalinga didžiųjų duomenų analizė, paremta efektyviausiais duomenų mokslo analizės metodais.

Tikimasi, kad atnaujinta elektroninių nusikaltimų tyrimo infrastruktūra bei įdiegti nauji tyrimo būdai sudarys sąlygas greičiau ir kokybiškiau ištirti nusikalstamas veikas.

2.2. Mažai dėmesio elektroninių nusikaltimų tyrėjų kompetencijų didinimui.

Naujos technologijos reikalauja peržiūrėti standartines veikimo procedūras (pvz., nusikaltimų įkalčių rinkimo), stiprinti ne tik nusikaltimų elektroninėje erdvėje tyrimus vykdančių institucijų, bet ir KSS bei YSII valdytojų bei tvarkytojų gebėjimus. Identifikuota, kad 64 proc. KSS nėra aišku, kaip įvertinti nusikaltimo nuostolį ar žalą, o 27 proc. – kaip reaguoti į galimai vykdomą nusikaltimą elektroninėje erdvėje[33]. Vis dėlto, įvertinant pateiktas rekomendacijas[34] ir atsižvelgiant į didėjantį nusikalstamų veikų techninį sudėtingumą, pirmiausia svarstytina intensyvinti nusikalstamas veikas užkardančio ir tiriančio personalo techninius gebėjimus. Siekiant problemą spręsti kompleksiškai, pirmiausiai reikia stiprinti institucijų, vykdančių nusikaltimų elektroninėje erdvėje tyrimus, pajėgumą ir nuosekliai pereiti prie KSS ir YSII valdytojų ir tvarkytojų pajėgumų stiprinimo.

Tikimasi, kad sudarytos sąlygos didinti elektroninių nusikaltimų tyrėjų kompetencijas leis juos apmokyti dirbti naujais būdais ir įrankiais.

3. Žemas visuomenės ir smulkaus bei vidutinio verslo žinių kibernetinio saugumo srityje lygis ir praktiniai gebėjimai jas pritaikyti.

Kiekvienas visuomenės narys ar organizacija turėtų suvokti jiems kylančias kibernetinio saugumo rizikas, mokėti jas kritiškai vertinti ir integruoti šį vertinimą į kasdienį sprendimų priėmimo procesą. Rizikų vertinimas yra esminis saugumo elementas, todėl rizikų nevertinimas prilygsta jų priėmimui pagal nutylėjimą, apima ir toleranciją potencialiai maksimaliai žalai, kuri ne visada suvokiama[35]. Nors skaitmeninė visuomenės atskirtis mažėja, atskirtis kibernetinio saugumo srityje tarp tų, kurie sugeba pasirūpinti savo kibernetiniu saugumu, ir tų, kurie negali, išlieka. Negebančius pasirūpinti kibernetiniu saugumu visuomenės narius galima skirstyti į įvairias grupes. Vertinama, kad tam tikros grupės, kaip senjorai, mažas pajamas turintys gyventojai ar užsieniečiai, gali patirti neproporcingai didelę žalą kibernetinės atakos atveju. Asmenys ir organizacijos neturi tapti kibernetinio saugumo specialistais, tačiau turi turėti bazinių kibernetinio saugumo žinių. Bazinės kibernetinio saugumo žinios ir kibernetinės higienos praktika, kaip atnaujinimų įdiegimas, sudėtingų slaptažodžių naudojimas, atsarginių kopijų darymas, daugeliu atvejų gali padėti išvengti kibernetinių atakų ir jų sukeliamos žalos.

Didesnių organizacijų didesnis kibernetinis atsparumas įprastai būna paremtas didesniais finansiniais resursais ir kompetentingais specialistais, tuo tarpu mažesnės organizacijos kibernetinio saugumo kompetencijų organizacijos viduje neaugina, tačiau gauna iš trečiųjų šalių. Trūksta pagalbos mažesnius

[32] Europol. *Internet organised crime threat assessment 2021*.
[33] Valstybės kontrolė. *Valstybinio audito ataskaita „Ar veiksingai kovojama su elektroniniais nusikaltimais*, 2020.
[34] Europol. *Internet organised crime threat assessment 2021*.
[35] OECD, *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, 2022.

resursus turinčioms organizacijoms vykdant kibernetinio saugumo žinių sklaidą. „Kurk Lietuvai“ vykdyto projekto metu[36] nustatyta, kad 60 proc. MVĮ neturi formaliai apibrėžtos ir reguliariai atnaujinamos kibernetinio saugumo politikos, net 79 proc. jų per 12 mėn. nevykdė įmonės kibernetinio saugumo rizikos vertinimo, o 74 proc. nepasiruošusios arba nežino, ar yra pasiruošusios atremti kibernetines atakas. MVĮ, kurios nesispecializuoja kibernetinio saugumo srityje, gali būti labiau pažeidžiamos kibernetinių incidentų atveju, nes veiksmingiems kibernetinio saugumo sprendimams įdiegti reikia didelių investicijų ir daug žinių.

MVĮ yra itin svarbios ne tik dėl didelės tikimybės tapti kibernetinių incidentų taikiniu, bet ir dėl galimybės sukurti ir pasiūlyti inovatyvių sprendimų, todėl sudarius sąlygas MVĮ dirbantiems asmenims įgyti žinių, skyrus jiems reikalingą pagalbą, būtų užtikrintas ne tik pakankamas kibernetinis atsparumas, tačiau ir MVĮ, aktyviai veikiančios kibernetinio saugumo srityje, galėtų prisidėti prie kibernetinio saugumo sprendinių valstybės mastu.

4. Nenustatytos viešojo ir privataus sektoriaus bendradarbiavimo kryptys.

Kibernetinio saugumo rinka, nors ir jauna, tačiau yra viena iš sparčiausiai augančių rinkų pasaulyje[37]. ES sukaupta daug ekspertinių žinių ir patirties kibernetinio saugumo mokslinių tyrimų, technologinės ir pramonės plėtros srityje ir nors ES atliekami pasaulinio lygio kibernetinio saugumo technologijų tyrimai, tačiau šios žinios per retai paverčiamos pasaulinio lygio kibernetinio saugumo produktais ir paslaugomis, tai lemia mažesnį konkurencingumą ir veiksmingumą tinklų ir informacinių sistemų apsaugos srityje.

ES kibernetinio saugumo įmonės susiduria su daugybe iššūkių bandydamos plėsti savo verslą. Jos pasižymi prastesniais rezultatais, palyginti su ne ES šalių kompanijomis: jų yra mažiau, jos paprastai pritraukia mažiau finansavimo, nepakankamai išvystytos produktų kūrimo galimybės, trūksta veiklos patirties, sudėtinga pasiekti tarptautines rinkas. Siekiant sukurti naują Europos kibernetinio saugumo inovacijų ekosistemą, buvo įsteigtas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas, kuris turėtų paskatinti Europos kibernetinio saugumo rinkos konkurencingumą ir stiprios Europos kibernetinio saugumo kompetencijų bendruomenės augimą ir brandą, stiprinti jos įgūdžius ir kompetencijas. Nacionalinio koordinavimo centras per 2 metus sieks suburti stabilią, efektyviai bendradarbiaujančią Lietuvos kibernetinio saugumo bendruomenę bei teikti paramą MVĮ, kad paskatintų jas naudoti bei kurti ir plėtoti naujausius kibernetinio saugumo sprendimus. Tikimasi, kad sukurta įvairialypė priemonių sistema sudarys sąlygas plėtoti kibernetinio saugumo sektoriaus inovacijas ir didinti kibernetinį atsparumą.

---

[36] Kurk Lietuvai, NKSC ir KAM. *Kibernetinis saugumas ir verslas*, 2020. http://kurklt.lt/wp-content/uploads/2020/06/Kibernetinis-saugumas-ir-verslas.-K%C4%85-tur%C4%97t%C5%B3-%C5%BEinoti-kiekvienas-%C4%AFmon%C4%97s-vadovas.pdf.

[37] European Investment Bank. *European Cybersecurity Investment Platform*, 2021, https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf.