Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/1101

2024 4 12

KOMISIJOS REKOMENDACIJA (ES) 2024/1101

2024 m. balandžio 11 d.

dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 292 straipsnį,

atsižvelgdama į 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvą (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 ([1]) (TIS 2 direktyvą),

kadangi:

(1) duomenų ir perduodamos neskelbtinos informacijos apsauga yra nepaprastai svarbi Sąjungos visuomenei, ekonomikai, saugumui ir gerovei. Kibernetinis saugumas yra strategiškai svarbus kuriant prie skaitmeninio amžiaus prisitaikiusią Europą ([2]) ir yra vienas iš pagrindinių Skaitmeninio dešimtmečio politikos programos ([3]) tikslų;

(2) ir ES saugumo sąjungos strategijoje ([4]), ir ES kibernetinio saugumo strategijoje ([5]) pabrėžiama, kad viena iš pagrindinių technologijų, padedančių užtikrinti atsparumą, technologinį suverenumą ir kibernetinių išpuolių prevencijai reikalingus operatyvinius pajėgumus, yra šifravimas. Skaitmeniniame pasaulyje šifravimas yra išties labai svarbus siekiant apsaugoti skaitmenines sistemas ir sandorius, įvairias pagrindines teises, taip pat užtikrinti gynybos pajėgumus. Įvairių šalių ir privačių subjektų lenktynės siekiant kurti kvantinės kompiuterijos pajėgumus ir atverti naujų potencialiai naudingų galimybių kelia grėsmę dabartiniams kriptografijos standartams. Šie standartai atlieka lemiamą vaidmenį užtikrinant duomenų konfidencialumą bei vientisumą ir perduodamos neskelbtinos informacijos apsaugą ir prisideda prie pagrindinių tinklo saugumo elementų;

(3) atsižvelgdama į tai, kad ateityje gali būti sukurti kvantiniai kompiuteriai, galintys nulaužti šiuolaikinį šifravimą, Europa turi ieškoti tvirtesnės apsaugos priemonių, kuriomis būtų užtikrinta perduodamos neskelbtinos informacijos apsauga ir ilgalaikis konfidencialios informacijos vientisumas, t. y. reikia kuo greičiau pereiti prie postkvantinės kriptografijos. Ši naujos rūšies kriptografija padės pašalinti žinomus trūkumus, kuriais pasižymi dabartinė asimetrinė kriptografija, ir padidinti atsparumą grėsmėms, kurias kelia piktavališkas kvantinių kompiuterių naudojimas;

(4) pripažindama galimą grėsmę, kurią kvantinė kompiuterija kelia kriptografijai viešuoju raktu, Komisija jau daugiau kaip dešimtmetį finansuoja postkvantinės kriptografijos srities mokslinius tyrimus ir plėtrą;

(5) valstybės narės turėtų apsvarstyti galimybę savo dabartinei viešojo administravimo institucijų skaitmeninei infrastruktūrai bei paslaugoms ir kitai ypatingos svarbos infrastruktūrai kuo greičiau pradėti taikyti postkvantinę kriptografiją, t. y. iš esmės pakeisti kriptografijos algoritmus, protokolus ir sistemas. Kaip pabrėžta neseniai paskelbtoje Komisijos baltojoje knygoje „Kaip patenkinti Europos skaitmeninės infrastruktūros poreikius?“, tam reikalingos koordinuotos valdžios institucijų, standartizacijos įstaigų, sektorių suinteresuotųjų subjektų, tyrėjų ir kibernetinio saugumo specialistų pastangos;

(6) siekiant užtikrinti suderintą ir vienalaikį perėjimą prie postkvantinės kriptografijos skirtingose valstybėse narėse ir jų valdžios sektoriuose, šioje Komisijos rekomendacijoje valstybės narės raginamos parengti išsamią postkvantinės kriptografijos įdiegimo strategiją. Šioje strategijoje turėtų būti nustatyti aiškūs galutiniai bei tarpiniai tikslai ir terminai, taigi nubrėžtos bendros perėjimo prie postkvantinės kriptografijos veiksmų gairės. Pagal jas visoje

([1]) OL L 333, 2022 12 27, p. 80.
([2]) COM(2020) 67 *final*.
([3]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos sprendimas (ES) 2022/2481, kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa (OL L 323, 2022 12 19, p. 4).
([4]) COM(2020) 605 *final*.
([5]) JOIN(2020) 18 *final*.

Sąjungoje į esamas viešojo administravimo sistemas ir ypatingos svarbos infrastruktūrą turėtų būti įdiegtos mišrios sistemos, derinančios postkvantinės kriptografijos technologijas su esamais kriptografijos metodais ar kvantiniu raktų paskirstymu;

(7) kad prie postkvantinės kriptografijos būtų pereita veiksmingai, Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairėse turėtų būti išvardyti reikalingi valstybių narių veiksmai, įskaitant postkvantinės kriptografijos algoritmų apsvarstymą, ir nurodyti aiškūs atskirų etapų ir tarpinių tikslų pasiekimo terminai, nustatyti atsižvelgiant į šių etapų ir tikslų tarpusavio priklausomybę ir į tai, kurie suinteresuotieji subjektai turėtų būti įtraukti;

(8) kad prie postkvantinės kriptografijos visoje Sąjungoje būtų pereita suderintai, labai svarbu parengti bendrus Europos standartus ir sukurti sistemą, pagal kurią būtų nustatomi ir atrenkami postkvantinės kriptografijos algoritmai, diegtini visų Sąjungos šalių skaitmeniniuose tinkluose ir paslaugose. Aktyviai dalyvaujant ES finansuojamiems mokslininkams, Sąjunga tarptautiniuose postkvantinės kriptografijos algoritmų atrankos procesuose jau padeda kurti ir bandyti potencialius standartuose nustatytinus postkvantinės kriptografijos algoritmus. Šioje Komisijos rekomendacijoje valstybės narės raginamos, ES lygmeniu glaudžiai bendradarbiaujant su Sąjungos kibernetinio saugumo ekspertais, TIS bendradarbiavimo grupe ir Europos Sąjungos kibernetinio saugumo agentūra (ENISA), vertinti postkvantinės kriptografijos algoritmus, atrinkti tinkamus ir juos patvirtinti kaip ES standartus, kad prie postkvantinės kriptografijos visoje Sąjungoje būtų pereita suderintai;

(9) kad ir toliau būtų išlaikytas ryšių sąveikumas, valstybės narės ir Sąjunga turėtų tęsti aktyvų tarptautiniams postkvantinės kriptografijos standartams parengti skirtą bendradarbiavimą su savo tarptautiniais strateginiais partneriais;

(10) valstybių narių sutartomis Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairėmis turėtų būti remiamasi rengiant nacionalinius perėjimo prie postkvantinės kriptografijos planus, o jei tokie planai jau parengti, jie turėtų būti suderinami su tomis bendromis Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairėmis;

(11) siekdama užtikrinti šios rekomendacijos tikslų įgyvendinimo pažangą, Komisija ketina atidžiai stebėti, kokių veiksmų pagal ją imamasi. Todėl valstybės narės raginamos, paprašytos Komisijos, pateikti jai visą tokiai stebėsenai užtikrinti reikalingą informaciją, kurios iš jų galima pagrįstai tikėtis. Remdamasi taip gauta ir visa kita turima informacija, Komisija įvertins šios rekomendacijos poveikį ir nuspręs, ar reikia imtis papildomų veiksmų, be kita ko, pasiūlyti privalomų Sąjungos teisės aktų;

(12) ši rekomendacija dėl postkvantinės kriptografijos grindžiama ES kibernetinio saugumo strategijoje nustatytais politikos tikslais didinti Sąjungos viešojo administravimo institucijų skaitmeninės infrastruktūros bei paslaugų ir kitos ypatingos svarbos infrastruktūros perdavimo linijų apsaugą ir atsparumą; ji atitinka bendrosios skaitmeninės rinkos ir bendro komunikato „Europos ekonominio saugumo strategija“ (10919/23) ([6]) tikslus; ja taip pat atsižvelgiama į ypatingos svarbos infrastruktūros fiziniam ir kibernetiniam saugumui kylančią riziką ir į grėsmes, nustatytas neseniai atlikus su kvantinėmis technologijomis susijusį rizikos vertinimą ([7]). Rekomendacija paisoma visų pirma ES pagrindinių teisių chartijoje (7, 8 ir 11 straipsniuose) ir Europos žmogaus teisių konvencijoje (8 ir 10 straipsniuose) pripažintų pagrindinių teisių ir principų, pagal kuriuos valdžios institucijoms tenka pozityvi pareiga mažinti neteisėtos prieigos prie informacijos ir jos kontrolės riziką, taigi būtinybė užtikrinti kriptografijos technologijų apsaugą ir skatinti jų naudojimą,

([6]) https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/lt/pdf.
([7]) JOIN(2023) 20 *final*.

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

1. TAIKYMO SRITIS IR TIKSLAI

Šios rekomendacijos tikslas – skatinti Sąjungoje pereiti prie postkvantinės kriptografijos, padedančios apsaugoti viešojo administravimo institucijų skaitmeninę infrastruktūrą bei paslaugas ir kitą ypatingos svarbos infrastruktūrą, sudarant valstybėms narėms sąlygas:

(1) nubrėžti Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gaires, kurių tikslas – sinchronizuoti valstybių narių pastangas parengti ir įgyvendinti nacionalinius tokio perėjimo planus, kartu užtikrinant tarpvalstybinį sąveikumą;

(2) padedant kibernetinio saugumo ekspertams, prisidėti prie postkvantinės kriptografijos ES algoritmų vertinimo, tinkamų algoritmų atrankos ir jų kaip Sąjungos standartų, įgyvendintinų visoje Sąjungoje pagal Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gaires, patvirtinimo;

(3) imtis tinkamų ir proporcingų priemonių, padedančių pasirengti šiam perėjimui.

2. KOORDINUOTŲ PERĖJIMO PRIE POSTKVANTINĖS KRIPTOGRAFIJOS VEIKSMŲ GAIRĖS

(4) Šia rekomendacija valstybės narės raginamos Sąjungos lygmeniu koordinuoti savo veiksmus per specialų valstybių narių forumą. Šiuo tikslu Komisija valstybėms narėms rekomenduoja naudotis esamomis Sąjungos lygmens kibernetinio saugumo srities struktūromis ir įsteigti TIS bendradarbiavimo grupės pogrupį. Šį pogrupį galėtų sudaryti nacionalinių saugumo agentūrų atstovai ir kibernetinio saugumo ekspertai visų pirma iš nacionalinių kibernetinio saugumo institucijų ir agentūros ENISA. Pogrupis gali pakviesti savo darbe dalyvauti atitinkamų suinteresuotųjų subjektų, kaip antai viešųjų organizacijų patariamųjų organų, sektorių subjektų, paslaugų teikėjų ir operatorių, atstovus, kad galėtų surinkti informaciją apie viešojo administravimo institucijų skaitmeninės infrastruktūros bei paslaugų ir kitos ypatingos svarbos infrastruktūros perėjimą prie postkvantinės kriptografijos įvairiuose sektoriuose ir šia informacija keistis, nacionaliniu lygmeniu koordinuoti tų subjektų veiksmus ir, laikydamasis Sąjungos konkurencijos taisyklių bei Sąjungos duomenų apsaugos teisės, parengti Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gaires.

(5) Šis postkvantinės kriptografijos pogrupis turėtų apsvarstyti, kokios priemonės būtų tinkamos, veiksmingos ir proporcingos siekiant apibrėžti Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių koncepciją ir koordinuoti jų rengimą. Kad būtų išvengta pastangų dubliavimosi ir užtikrintas nuoseklus požiūris į tai, kaip spręsti kylančias problemas, postkvantinės kriptografijos pogrupis raginamas diskutuoti su kitomis atitinkamomis įstaigomis, kaip antai Europolu, NATO ir kt.

(6) Todėl valstybės narės raginamos netrukus po šios rekomendacijos paskelbimo įsteigti tokį postkvantinės kriptografijos pogrupį pagal Komisijos įgyvendinimo sprendimą (ES) 2017/179 ([8]) ir paskirti atstovus ekspertus, kurie turėtų glaudžiai bendradarbiauti su Komisija ir kuriems turėtų būti pavesta apibrėžti Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių koncepciją ir jas parengti.

(7) Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairės turėtų būti parengtos per dvejus metus nuo šios rekomendacijos paskelbimo, o tada, laikantis jose nustatytų principų, bus parengti ir tinkamai pritaikyti atskirų valstybių narių perėjimo prie postkvantinės kriptografijos planai.

3. SĄJUNGOS LYGMENS VEIKSMAI

(8) Visą darbą, bendradarbiaudama su valstybių narių atstovais ekspertais, stebės ir periodiškai vertins Komisija.

([8]) 2017 m. vasario 1 d. Komisijos įgyvendinimo sprendimas (ES) 2017/179, kuriuo pagal Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti 11 straipsnio 5 dalį nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti (OL L 28, 2017 2 2, p. 73).

(9) Šiuo tikslu Komisija gali paprašyti valstybių narių atstovų pateikti jai visą pažangos, pasiektos rengiant Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gaires, ir numatytų priemonių veiksmingumo stebėsenai užtikrinti reikalingą informaciją, kurios iš jų galima pagrįstai tikėtis.

(10) Remdamasi ta ir visa kita turima informacija, Komisija įvertins numatytas priemones ir valstybių narių atstovų tinklo veikimą ir nuspręs, ar reikia imtis papildomų veiksmų, be kita ko, pasiūlyti privalomų Sąjungos teisės aktų.

4. **PERŽIŪRA**

(11) Valstybės narės turėtų bendradarbiauti su Komisija, kad ne vėliau nei per trejus metus nuo rekomendacijos paskelbimo būtų įvertintas jos poveikis ir nustatyti tinkami tolesni veiksmai. Atliekant šį vertinimą turėtų būti atsižvelgiama į postkvantinės kriptografijos pogrupio, sudaryto iš nacionalinių ekspertų, darbo rezultatus.

Priimta Briuselyje 2024 m. balandžio 11 d.

Komisijos vardu
Thierry BRETON
Komisijos narys