Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/2392

2025 12 1

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/2392

2025 m. lapkričio 28 d.

dėl svarbių ir ypatingos svarbos produktų su skaitmeniniais elementais kategorijų techninio aprašymo pagal Europos Parlamento ir Tarybos reglamentą (ES) 2024/2847

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentą (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828, (Kibernetinio atsparumo aktas) ([1]), ypač į jo 7 straipsnio 4 dalį,

kadangi:

(1) Reglamentu (ES) 2024/2847 nustatomos kibernetinio saugumo taisyklės, taikomos produktams su skaitmeniniais elementais. Visų pirma to reglamento III priede nustatyta, kurių kategorijų svarbiems produktams su skaitmeniniais elementais, tiekiamiems rinkai, taikomos atitikties vertinimo procedūros yra griežtesnės už procedūras, taikomas kitiems produktams su skaitmeniniais elementais. Reglamento (ES) 2024/2847 IV priede nustatyta, kurių kategorijų ypatingos svarbos produktų su skaitmeniniais elementais gamintojams gali būti taikomas reikalavimas gauti Europos kibernetinio saugumo sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 ([2]), arba kurių tokių rinkai tiekiamų produktų atitiktį privalomai turi įvertinti trečioji šalis;

(2) pagal Reglamento (ES) 2024/2847 7 straipsnio 1 dalį ir 8 straipsnio 1 dalį, nuo produkto su skaitmeniniais elementais pagrindinės funkcijos priklauso tai, ar produktas su skaitmeniniais elementais atitinka svarbių ar ypatingos svarbos produktų su skaitmeniniais elementais kategorijos techninį aprašą, vadinasi, ir taikytinos atitikties vertinimo procedūros;

(3) kad kurdami produktą su skaitmeniniais elementais įdiegtų pageidaujamų funkcijų derinį, gamintojai į savo produktus su skaitmeniniais elementais paprastai integruoja kitus komponentus, kurie savo ruožtu taip pat yra produktai su skaitmeniniais elementais ir gali atitikti svarbių ar ypatingos svarbos produktų kategorijos techninį aprašą. Pagal Reglamentą (ES) 2024/2847, svarbiems ir ypatingos svarbos produktams su skaitmeniniais elementais nustatytos atitikties vertinimo procedūros yra taikomos produktui su skaitmeniniais elementais, jei visas toks produktas yra svarbus arba ypatingos svarbos produktas, įrašytas į to reglamento III ir IV priedus. Pavyzdžiui, jei į išmaniojo telefono mobiliąją naujienų programėlę yra įterpta interneto naršyklė, tai savaime nereiškia, kad naujienų programėlei turi būti pritaikyta atitikties vertinimo procedūra, numatyta produktams su skaitmeniniais elementais, kurie pagal savo pagrindinę funkciją yra „atskiros ir įterptosios naršyklės“. Tačiau pagal Reglamentą (ES) 2024/2847 gamintojas turi užtikrinti, kad visas produktas su skaitmeniniais elementais atitiktų esminius kibernetinio saugumo reikalavimus. Todėl gamintojas viso produkto saugumą turi įvertinti atsižvelgdamas į atitinkamai komponentų arba funkcijų, įdiegtų į tą produktą, saugumą. Pavyzdžiui, mobiliosios naujienų programėlės gamintojas, kad įrodytų savo produkto su skaitmeniniais elementais atitiktį Reglamentui (ES) 2024/2847, turi įrodyti, kad taikytinus reikalavimus atitinka visa mobilioji naujienų programėlė, atsižvelgiant atitinkamai į interneto naršyklės, įterptos į tą programėlę, saugumą;

([1]) OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) aplinkybė, kad produktas su skaitmeniniais elementais turi funkcijų, nenurodytų šio reglamento techniniuose aprašuose, arba turi tas aprašuose nurodytas funkcijas papildančių funkcijų, savaime nereiškia, kad produktas su skaitmeniniais elementais neturi Reglamento (ES) 2024/2847 III ir IV prieduose nustatytos produktų kategorijos pagrindinės funkcijos. Pavyzdžiui, produktuose su skaitmeniniais elementais, kurie pagal savo pagrindinę funkciją yra „operacinės sistemos“, dažnai būna programinė įranga, atliekanti pagalbines į produkto kategorijos techninį aprašą neįtrauktas funkcijas, pavyzdžiui, skaičiuotuvas arba grafikos rengyklė. Produktuose su skaitmeniniais elementais dažnai būna komponentų, turinčių kito svarbaus ar ypatingos svarbos produkto su skaitmeniniais elementais funkcijų, pavyzdžiui, operacinę sistemą su integruotomis interneto naršyklės funkcijomis arba maršruto parinktuvą su užkardos funkcijomis. Vis dėlto tai savaime nereiškia, kad tokie produktai su skaitmeniniais elementais neturi pagrindinių atitinkamai „operacinės sistemos“ arba „maršruto parinktuvo, modemo, skirto prisijungti prie interneto, ir jungiklio“ funkcijų;

(5) kita vertus, jei produktas su skaitmeniniais elementais gali atlikti Reglamento (ES) 2024/2847 III ir IV prieduose nustatytų kategorijų produktų funkcijas, tačiau jo paties pagrindinė funkcija skiriasi nuo tokios kategorijos produktų pagrindinės funkcijos, toks produktas nelaikomas atitinkančiu tos kategorijos produktų techninį aprašą. Pavyzdžiui, saugumo suderinimo, automatizavimo ir reagavimo programinė įranga (angl. *security orchestration, automation and response*, SOAR) dažnai gali atlikti kategorijos „saugumo informacijos ir įvykių valdymo (SIEM) sistemos“ produktų su skaitmeniniais elementais funkcijas, t. y. rinkti duomenis, juos analizuoti ir pateikti kaip informaciją, kuria remiantis pritaikomos saugumo priemonės. Tačiau, atsižvelgiant į tai, kad SOAR programinės įrangos pagrindinės funkcijos nėra SIEM funkcijos, tokia programinė įranga nelaikoma atitinkančia kategorijos „saugumo informacijos ir įvykių valdymo (SIEM) sistemos“ techninį aprašą. Panašiai išmaniajame telefone būna komponentų, atliekančių kelių Reglamento (ES) 2024/2847 III ir IV prieduose nustatytų kategorijų produktų, pavyzdžiui, operacinės sistemos arba įdiegtos slaptažodžių tvarkytuvės, funkcijas. Tačiau pagrindinė išmaniojo telefono funkcija nėra tokia kaip operacinės sistemos arba slaptažodžių tvarkytuvės, todėl jis paprastai neturėtų būti laikomas atitinkančiu tokių kategorijų produktų techninius aprašus;

(6) pagal Reglamento (ES) 2024/2847 13 straipsnio 2 ir 3 dalis, produktų su skaitmeniniais elementais gamintojai turi užtikrinti, kad Reglamento (ES) 2024/2847 I priedo I dalyje nustatytų esminių kibernetinio saugumo reikalavimų laikymasis būtų proporcingas produkto su skaitmeniniais elementais rizikai ir pagrįstas numatytąja paskirtimi ir pagrįstai numatomu naudojimu, taip pat produkto su skaitmeniniais elementais naudojimo sąlygomis, atsižvelgiant į tikėtiną produkto naudojimo laikotarpį. Nesvarbu, ar produktas su skaitmeniniais elementais laikomas svarbiu ar ypatingos svarbos produktu su skaitmeniniais elementais, gamintojai pagal minėto reglamento 13 straipsnio 2 ir 3 dalis turi atlikti išsamų kibernetinio saugumo rizikos vertinimą ir nurodyti, kaip kibernetinio saugumo reikalavimai įgyvendinami remiantis rizikos vertinimu, įskaitant jų atliekamus bandymus ir teikiamas garantijas. Jei produkto su skaitmeniniais elementais pagrindinė funkcija atitinka svarbaus ar ypatingos svarbos produkto su skaitmeniniais elementais techninį aprašą, gamintojai atitiktį turi įrodyti laikydamiesi Reglamento (ES) 2024/2847 32 straipsnio 2, 3, 4 ir 5 dalyse nustatytų konkrečių atitikties vertinimo procedūrų;

(7) šiame reglamente pateikti pavyzdžiai, kokie būna produktai su skaitmeniniais elementais, kurių pagrindinės funkcijos atitinka tam tikrų svarbių ar ypatingos svarbos produktų su skaitmeniniais elementais techninį aprašą. Tokie pavyzdžiai pateikiami dėl aiškumo, o jų sąrašas nėra baigtinis;

(8) siekiant užtikrinti teisinį tikrumą gamintojams, tokių produktų su skaitmeniniais elementais, kaip klastojimui atsparūs mikroprocesoriai, klastojimui atsparūs mikrovaldikliai ir išmaniosios kortelės bei panašūs prietaisai, įskaitant saugiuosius elementus, kategorijos turėtų būti atskirtos priklausomai nuo atsparumo bandymams išnaudoti spragas arba ydas, į kurį orientuojantis tie produktai buvo suprojektuoti. Plačiai naudojamas ir standartizuotas būdas tokiam atsparumo lygiui išreikšti yra AVA_VAN lygis. AVA_VAN lygiai yra apibrėžti viešai prieinamuose bendrųjų kriterijų ir bendrosios vertinimo metodikos standartuose, kuriais grindžiami dabartiniai rinkoje priimti pagrindiniai sertifikavimo reikalavimai, pavyzdžiui, Komisijos įgyvendinimo reglamentas (ES) 2024/482 ([3]). Įgyvendinimo

([3]) 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo, (OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

reglamentu (ES) 2024/482 nustatyta Europos kibernetinio saugumo sertifikavimo schema, kuria galima remtis siekiant produktą sertifikuoti konkrečiu saugumo užtikrinimo lygiu. Atsižvelgus į pasaulinę praktiką, Įgyvendinimo reglamente (ES) 2024/482 numatyta galimybė sertifikatus iki 2027 m. išduoti remiantis ankstesnėmis standartų redakcijomis. Todėl dera leisti, taikant Reglamentą (ES) 2024/2847, AVA_VAN lygius išreikšti nuorodomis arba į naujausią, arba į ankstesnes tų standartų redakcijas;

(9) šiame reglamente nustatytos priemonės atitinka pagal Reglamento (ES) 2024/2847 62 straipsnio 1 dalį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) bendrieji kriterijai – bendrieji informacinių technologijų saugumo vertinimo kriterijai, apibrėžti Įgyvendinimo reglamento (ES) 2024/482 2 straipsnio 1 punkte arba to įgyvendinimo reglamento 3 straipsnio 2 dalies a ir b punktuose nurodytuose standartuose;

2) bendroji vertinimo metodika – bendroji informacinių technologijų saugumo vertinimo metodika, apibrėžta Įgyvendinimo reglamento (ES) 2024/482 2 straipsnio 2 punkte arba to įgyvendinimo reglamento 3 straipsnio 2 dalies c ir d punktuose nurodytuose standartuose.

2 straipsnis

1. Reglamento (ES) 2024/2847 III priede išvardytų I ir II klasės produktų su skaitmeniniais elementais kategorijų techninis aprašas pateikiamas šio reglamento I priede.

2. Reglamento (ES) 2024/2847 IV priede išvardytų produktų su skaitmeniniais elementais kategorijų techninis aprašas pateikiamas šio reglamento II priede.

3 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2025 m. lapkričio 28 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

SVARBŪS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS

I klasė

Produktų kategorija	Techninis aprašas
1. Tapatybės valdymo sistemos ir privilegijuotos prieigos valdymo programinė ir aparatinė įranga, įskaitant tapatumo nustatymo ir prieigos kontrolės skaitytuvus, be kita ko, biometrinius skaitytuvus	Tapatybės valdymo sistemos – produktai su skaitmeniniais elementais, kuriais užtikrinami tapatumo nustatymo arba leidimų suteikimo mechanizmai, taip pat fizinių asmenų, juridinių asmenų, įrenginių arba sistemų tapatybės kredencialų valdymo per visą gyvavimo ciklą, pavyzdžiui, tapatybės užregistravimo, administravimo, priežiūros ir išregistravimo, mechanizmai. Prie tokių sistemų priskiriamos fizinių asmenų, juridinių asmenų, įrenginių arba sistemų prieigos prie skaitmeninių išteklių arba fizinių vietų valdymo sistemos. Privilegijuotos prieigos valdymo programinė įranga yra prieigos valdymo sistema, kuria valdomos ir stebimos prieigos prie informacinių arba operacinių technologijų (IT arba OT) sistemų ir neskelbtinų duomenų teisės organizacijoje; prie tokių sistemų priskiriamos sistemos, kuriomis užtikrinama diferencijuotos prieigos kontrolės politika, taikoma privilegijuotiems naudotojams. Prie šios kategorijos, be kita ko, priskiriami tapatumo nustatymo ir prieigos kontrolės skaitytuvai, biometriniai skaitytuvai, vieno prisijungimo programinė įranga, susietosios tapatybės valdymo programinė įranga, vienkartinių slaptažodžių programinė įranga, aparatiniai tapatumo nustatymo įrenginiai, pavyzdžiui, operacijos autentifikavimo kodų (angl. *transaction authentication number*, TAN) generatoriai, tapatumo patvirtinimo programinė įranga ir daugiaveiksnio tapatumo nustatymo programinė įranga.
2. Atskiros ir įterptosios naršyklės	Programinės įrangos produktai su skaitmeniniais elementais, būtini tam, kad prie tinklų, pavyzdžiui, interneto, prijungtuose serveriuose laikomas žiniatinklio turinys ir paslaugos būtų prieinami bei teikiami galutiniams naudotojams ir kad būtų įmanoma tokių naudotojų ir turinio bei paslaugų sąveika. Tokiuose produktuose paprastai yra naršyklės variklis ženklinimo kalba (pavyzdžiui, HTML) parašytam turiniui interpretuoti ir rodyti, kuris yra pritaikytas veikti su žiniatinklio protokolais (pavyzdžiui, HTTP, HTTPS) ir gali įvykdyti scenarijus bei valdyti naudotojo įvestį, taip pat saugoti laikinus arba nuolatinius svetainių duomenis (slapukus). Prie šios kategorijos, be kita ko, priskiriamos naršyklių funkcijas atliekančios atskiros taikomosios programos, įterptosios naršyklės, skirtos integruoti į kitą sistemą arba taikomąją programą, taip pat žiniatinklio naršyklės, į kurias integruotas dirbtinio intelekto agentas.
3. Slaptažodžių tvarkyklės	Produktai su skaitmeniniais elementais, kuriuose slaptažodžiai laikomi pačiame įrenginyje (vietoje) arba nuotoliniame serveryje; jais taip pat atliekami tokie veiksmai kaip slaptažodžių generavimas ir dalijimasis slaptažodžiais, taip pat jie integruojami į vietines arba trečiosios šalies taikomąsias slaptažodžių naudojimo programas. Prie šios kategorijos, be kita ko, priskiriamos vietinės slaptažodžių tvarkytuvės, slaptažodžių tvarkytuvės, pateikiamos kaip naršyklės plėtiniai, organizacijos lygio slaptažodžių tvarkytuvės, taip pat aparatinės slaptažodžių tvarkytuvės.

Produktų kategorija	Techninis aprašas
4. Kenkimo programinės įrangos paieškos, šalinimo arba izoliavimo programinė įranga	Programinės įrangos produktai su skaitmeniniais elementais (kitaip – apsaugos nuo virusų arba kenkėjiškos programinės įrangos programos) įrenginiuose aptinka kenkėjišką programinę įrangą ar kodą arba pašalina ar izoliuoja tokią programinę įrangą ar kodą, kad įrenginiuose būtų išlaikytas integralumas, slaptumas arba tokių įrenginių prieinamumas. Šioje produktų kategorijoje kenkėjiška programinė įranga – programinė įranga, kurioje yra kenkėjiškų funkcijų arba priemonių, galinčių tiesiogiai arba netiesiogiai padaryti žalos naudotojui ir (arba) kompiuterinei sistemai, pavyzdžiui, virusai, kirminai, išpirkos reikalavimo programinė įranga ir Trojos arkliai. Prie šios kategorijos, be kita ko, priskiriama programinė įranga, kuri tikruoju laiku arba sureguliuota rankiniu būdu aptinka kenkėjišką programinę įrangą arba jos ieško, šerdinių kenkimo programų (*rootkit*) aptikimo ir sistemos atkūrimo diskai, kurių pagrindinė funkcija yra kenkėjiškos programinės įrangos paieška, jos pašalinimas arba izoliavimas.
5. Produktai su skaitmeniniais elementais, atliekantys virtualiojo privataus tinklo (VPN) funkciją	Produktai su skaitmeniniais elementais, sukuriantys užšifruotą loginį tunelį, sudarytą iš fizinio arba virtualiojo tinklo sisteminių išteklių. Prie šios kategorijos, be kita ko, priskiriami virtualiojo privačiojo tinklo klientai, virtualiojo privačiojo tinklo serveriai ir virtualiojo privačiojo tinklo sietuvai.
6. Tinklo valdymo sistemos	Produktai su skaitmeniniais elementais, kuriais prijungtieji tinklo elementai, pavyzdžiui, serveriai, maršruto parinktuvai, perjungikliai, darbo vietos, spausdintuvai arba nešiojamieji prietaisai, administruojami juos stebint ir valdant jų veikimą tinkle bei konfigūraciją. Prie šios kategorijos, be kita ko, priskiriamos ištisinio valdymo sistemos, konfigūracijos valdymo specialiosios sistemos, pavyzdžiui, programiškai valdomo tinklo valdikliai.
7. Saugumo informacijos ir įvykių valdymo (SIEM) sistemos	Produktai su skaitmeniniais elementais, kuriais duomenys iš daugybės šaltinių surenkami, analizuojami bei susiejami ir pateikiami kaip informacija, kuria remiantis pritaikomos saugumo priemonės, pavyzdžiui, grėsmės ir incidento aptikimo, ekspertinės analizės arba atitikties užtikrinimo tikslais.
8. Sistemos paleidimo tvarkyklės	Programinės įrangos produktai su skaitmeniniais elementais, kuriais pradinis sistemos paleidimas po įrenginio įjungimo / pakartotinio paleidimo valdomas inicijuojant aparatinę įrangą, įkeliant sistemą arba perduodant valdymą į operacinės sistemos aplinką arba sistemos ištekliams ir kuriais pasirenkami pradinio sistemos įkėlimo variantai. Prie šios kategorijos, be kita ko, priskiriama UEFI aparatinė programinė įranga, vienos arba kelių pakopų pradinio įkėlimo programos.
9. Viešojo rakto infrastruktūra ir skaitmeninių sertifikatų išdavimo programinė įranga	Produktai su skaitmeniniais elementais, kuriais viešųjų raktų infrastruktūroje (PKI) valdomas skaitmeninių sertifikatų patvirtinimas, kūrimas, išdavimas, platinimas, statuso skelbimas, galiojimo pratęsimas arba panaikinimas arba kuriais vykdomas su tokiais skaitmeniniais sertifikatais susijusių šifravimo raktų generavimas, saugojimas, deponavimas, dalijimasis jais, sunaikinimas arba reguliarus pakeitimas. Prie šios kategorijos, be kita ko, priskiriamos raktų valdymo sistemos, skaitmeninių sertifikatų valdymo sistemos, sertifikatų galiojimo patikros protokolo atsakikliai ir kompleksiniai PKI sprendiniai.

Produktų kategorija	Techninis aprašas
10. Fizinės ir virtualiosios tinklo sąsajos	Fizinės tinklo sąsajos – produktai su skaitmeniniais elementais, kuriais įrenginys prie tinklo tiesiogiai prijungiamas per programų sąsają (API), užtikrinamą sąsajos tvarkyklėmis, paprastai veikiančiomis kanalų lygmeniu, ir kurie turi aparatinės įrangos adapterius perdavimo terpėms su atitinkama mikroprogramine įranga, paprastai veikiančia fiziniu ir kanalų lygmeniu. Virtualios tinklo sąsajos – produktai su skaitmeniniais elementais, kuriais įrenginys prie tinklo tiesiogiai arba netiesiogiai prijungiamas per API, imituojančią fizinių tinklo sąsajų API tvarkykles, paprastai veikiančias kanalų lygmeniu. Prie šios kategorijos, be kita ko, priskiriamos laidinės ir belaidės tinklo plokštės, valdikliai ir adapteriai, pavyzdžiui, Wi-Fi, eterneto, IrDA, USB, *Bluetooth*, *NearLink*, *Zigbee* arba objekto magistralės, taip pat grynai virtualūs pavieniai produktai, pavyzdžiui, virtualios tinklo plokštės, tinklo sąsajos konteineriams ir VPN sąsajos.
11. Operacinės sistemos	Programinės įrangos produktai su skaitmeniniais elementais, kuriais užtikrinama abstrakti pagrindinės aparatinės įrangos sąsaja ir kuriais valdomas programinės įrangos vykdymas; be to, tokiais produktais gali būti teikiamos paslaugos, pavyzdžiui, valdomi ir konfigūruojami kompiuterio ištekliai, vykdomas planavimas, valdoma įvestis ir išvestis, valdomi duomenys, taip pat užtikrinama sąsaja, per kurią taikomosios programos sąveikauja su sistemos ištekliais ir periferiniais įrenginiais. Prie šios kategorijos, be kita ko, priskiriamos tikralaikės operacinės sistemos, bendrinės ir specialiosios operacinės sistemos.
12. Maršruto parinktuvai, modemai, skirti prisijungti prie interneto, ir jungikliai	Maršruto parinktuvai – paprastai tinklo lygiu veikiantys produktai su skaitmeniniais elementais, kuriais duomenų srautai tarp įvairių tinklų nustatomi ir valdomi parinktais keliais arba maršrutais, tam panaudojant maršruto parinkimo protokolus ir algoritmus. Prie šios kategorijos, be kita ko, priskiriami laidiniai ir belaidžiai maršruto parinktuvai, virtualūs maršruto parinktuvai ir maršruto parinktuvai su modemais arba be jų.
	Jungtis prie interneto skirti modemai – aparatinės įrangos produktai su skaitmeniniais elementais, kuriuose skaitmeninio moduliavimo ir demoduliavimo metodais analoginis signalas paverčiamas skaitmeniniu ir atvirkščiai, kad būtų galima užtikrinti IP grindžiamą ryšį. Prie šios kategorijos, be kita ko, priskiriami šviesolaidiniai modemai, skaitmeninės abonento linijos (DSL) modemai, laidiniai (DOCSIS) modemai, palydoviniai modemai ir mobiliojo ryšio modemai.
	Perjungtuvai (jungikliai) – valdymo matricą (programinę įrangą ir sąsajas) turintys paprastai duomenų ryšio arba tinklo lygiu įdiegiami produktai su skaitmeniniais elementais, kuriais jungtys tarp tinklo įrenginių užtikrinamos persiunčiant duomenų paketus. Prie šios kategorijos, be kita ko, priskiriami administruojamieji perjungtuvai, išmanieji perjungtuvai, daugiasluoksniai perjungtuvai, virtualieji saugumo perjungtuvai, programuojamieji perjungtuvai programiškai valdomam tinklui ir tinklų tiltai, pavyzdžiui, belaidės prieigos taškai.

Produktų kategorija	Techninis aprašas
13. Mikroprocesoriai, turintys su saugumu susijusių funkcijų	Produktai su skaitmeniniais elementais, kurie yra pagrindines apdorojimo funkcijas atliekantys integriniai grandynai, priklausomi nuo išorinės atminties ir periferinių įrenginių, įskaitant mikroprogramas ir kitą žemojo lygmens aparatinę programinę įrangą. Be to, jie atlieka su saugumu susijusias, pavyzdžiui, šifravimo, tapatybės patvirtinimo, saugaus raktų saugojimo, atsitiktinių skaičių generavimo, patikimos vykdymo aplinkos, funkcijas arba užtikrina kitus aparatine įranga pagrįstus apsaugos mechanizmus; taip apsaugomas ne vien pats mikroprocesorius, bet ir kiti produktai, tinklai arba paslaugos, pavyzdžiui, pradinio įkėlimo seka, virtualizavimas arba saugaus ryšio sąsajos.
14. Mikrovaldikliai, turintys su saugumu susijusių funkcijų	Produktai su skaitmeniniais elementais, kurie yra pagrindines apdorojimo funkcijas atliekantys integriniai grandynai su integruota atmintimi (todėl mikrovaldiklį galima užprogramuoti) ir paprastai su kitais periferiniais įrenginiais, įskaitant mikroprogramas ir kitą žemojo lygmens aparatinę programinę įrangą. Be to, jie atlieka su saugumu susijusias, pavyzdžiui, šifravimo, tapatybės patvirtinimo, saugaus raktų saugojimo, atsitiktinių skaičių generavimo, patikimos vykdymo aplinkos, funkcijas arba užtikrina kitus aparatine įranga pagrįstus apsaugos mechanizmus; taip apsaugomas ne vien pats mikrovaldiklis, bet ir kiti produktai, tinklai arba paslaugos, pavyzdžiui, pradinio įkėlimo seka, virtualizavimas arba saugaus ryšio sąsajos.
15. Konkrečios paskirties integriniai grandynai (ASIC) ir programuojamosios loginės matricos (FPGA), turinčios su saugumu susijusių funkcijų	Konkrečios paskirties integriniai grandynai (ASIC), turintys su saugumu susijusių funkcijų, yra tie produktai su skaitmeniniais elementais, kurie yra integriniai grandynai, visiškai arba iš dalies specialiai sukurti konkrečiai funkcijai atlikti arba konkrečiai prietaikai įdiegti, įskaitant mikroprogramas ir kitą žemojo lygmens aparatinę programinę įrangą. Be to, jie atlieka su saugumu susijusias, pavyzdžiui, šifravimo, tapatybės patvirtinimo, saugaus raktų saugojimo, atsitiktinių skaičių generavimo, patikimos vykdymo aplinkos, funkcijas arba užtikrina kitus aparatine įranga pagrįstus apsaugos mechanizmus; taip apsaugomas ne vien pats ASIC, bet ir kiti produktai, tinklai arba paslaugos, pavyzdžiui, pradinio įkėlimo seka, virtualizavimas arba saugaus ryšio sąsajos.
	Programuojamosios loginės matricos (FPGA), turinčios su saugumu susijusių funkcijų, yra tie produktai su skaitmeniniais elementais, kurie yra integriniai grandynai su jiems būdinga konfigūruojamų loginių blokų matrica ir kurie sukurti taip, kad juos pagamintus būtų galima užprogramuoti konkrečiai funkcijai atlikti arba konkrečiai prietaikai įdiegti, įskaitant mikroprogramas ir kitą žemojo lygmens aparatinę programinę įrangą. Be to, jie atlieka su saugumu susijusias, pavyzdžiui, šifravimo, tapatybės patvirtinimo, saugaus raktų saugojimo, atsitiktinių skaičių generavimo, patikimos vykdymo aplinkos, funkcijas arba užtikrina kitus aparatine įranga pagrįstus apsaugos mechanizmus; taip apsaugoma ne vien pati FPGA, bet ir kiti produktai, tinklai arba paslaugos, pavyzdžiui, pradinio įkėlimo seka, virtualizavimas arba saugaus ryšio sąsajos.
16. Išmanieji namų bendrosios paskirties virtualūs asistentai	Produktai su skaitmeniniais elementais, kurie, palaikydami ryšį viešajame internete tiesiogiai arba per kitą įrangą, apdoroja natūraliosios kalbos komandomis, pavyzdžiui, per garsinę arba rašytinę įvestį, pateiktas užklausas, užduotis arba klausimus ir kurie pagal tas užklausas, užduotis arba klausimus suteikia prieigą prie kitų paslaugų arba prie buityje naudojamų prijungtųjų įrenginių valdymo funkcijų. Prie šios kategorijos, be kita ko, priskiriami išmanieji garsiakalbiai su įdiegtu virtualiuoju asistentu ir šį aprašymą atitinkantys atskiri virtualieji asistentai.

Produktų kategorija	Techninis aprašas
17. Išmanieji namų produktai, turintys su saugumu susijusių funkcijų, įskaitant išmaniąsias durų spynas, saugumo kameras, kūdikių stebėjimo sistemas ir signalizacijos sistemas	Produktai su skaitmeniniais elementais, kuriais užtikrinamas fizinis vartotojų saugumas gyvenamojoje aplinkoje ir kuriuos galima valdyti arba administruoti nuotoliu kitomis sistemomis, taip pat aparatinė ir programinė įranga, kuriomis centralizuotai valdomi tokie produktai. Prie šios kategorijos, be kita ko, priskiriami išmanieji durų užraktai, kūdikių stebėjimo sistemos, signalizacijos sistemos ir namų apsaugos kameros.
18. Prie interneto prijungti žaislai, kuriems taikoma Europos Parlamento ir Tarybos direktyva 2009/48/EB ([1]) ir kurie turi socialinių interaktyvių funkcijų (pavyzdžiui, kalbėjimo ar filmavimo) arba buvimo vietos sekimo funkcijų	Prie interneto prijungti žaislai su interaktyvaus bendravimo funkcijomis yra produktai su skaitmeniniais elementais, kuriems taikoma Direktyva 2009/48/EB; tokiuose žaisluose, ryšį viešajame internete palaikančiuose tiesiogiai arba per kitą įrangą, įdiegtomis technologijomis priimama arba siunčiama, pavyzdžiui, klaviatūros, mikrofono, garsiakalbio arba fotoaparato, informacija.
	Prie interneto prijungti žaislai su buvimo vietos sekimo funkcijomis yra produktai su skaitmeniniais elementais, kuriems taikoma Direktyva 2009/48/EB; tokiuose žaisluose, ryšį viešajame internete palaikančiuose tiesiogiai arba per kitą įrangą, įdiegtomis technologijomis sekama arba nuspėjama žaislo arba jo naudotojo geografinė buvimo vieta. Jei žaislas jutiklių technologijomis tik aptinka tai, kad greta yra naudotojas arba kiti žaislai, nelaikoma, kad toks žaislas turi buvimo vietos sekimo funkcijų.
19. Asmeniniai dėvimi gaminiai, kurie yra dėvimi arba tvirtinami ant žmogaus kūno ir kurie turi sveikatos stebėsenos (pavyzdžiui, sekimo) paskirtį bei kuriems netaikomas Reglamentas (ES) 2017/745 ([2]) arba Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 ([3]), arba asmeniniai dėvimi gaminiai, kurie skirti naudoti vaikams	Asmeniniai dėvimi gaminiai, kurie dėvimi arba tvirtinami ant žmogaus kūno ir kurie turi sveikatos stebėjimo paskirtį, yra produktai su skaitmeniniais elementais, kurie ant žmogaus kūno dėvimi tiesiai arba per drabužius ar kitus reikmenis ir kurie reguliariai arba nuolat fiksuoja ir toliau apdoroja informaciją, įskaitant naudotojo sveikatai aktualius gyvybinius kūno parametrus; prie tokių gaminių nepriskiriami gaminiai, patenkantys į Reglamento (ES) 2017/745 arba Reglamento (ES) 2017/746 taikymo sritis. Prie šios kategorijos, be kita ko, priskiriami fizinio aktyvumo sekikliai, išmanieji laikrodžiai, išmanieji papuošalai, išmanieji drabužiai ir aprašą atitinkanti sportinė apranga.
	Asmeniniai dėvimi gaminiai, kuriuos naudos vaikai ir kurie yra skirti vaikams, yra produktai su skaitmeniniais elementais, kuriuos dėvėti ant kūno, tiesiai arba per drabužius ar kitus reikmenis, gali jaunesni kaip 14 metų asmenys. Prie šios kategorijos, be kita ko, priskiriami vaikiški dėvimieji saugos prietaisai.

([1]) 2009 m. birželio 18 d. Europos Parlamento ir Tarybos direktyva 2009/48/EB dėl žaislų saugos (OL L 170, 2009 6 30, p. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB, (OL L 117, 2017 5 5, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES, (OL L 117, 2017 5 5, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

II klasė

Produktų kategorija	Techninis aprašas
1. Hipervizoriai ir konteinerių paleidimo sistemos, padedantys virtualizuoti operacines sistemas ir panašias aplinkas	Hipervizoriai yra programinės įrangos produktai su skaitmeniniais elementais, kurie sukuria abstraktųjį skaičiavimo išteklių sluoksnį ir (arba) paskirsto tuos išteklius, todėl galima kurti, valdyti ir koordinuoti virtualias mašinas, logiškai atskirtas viena nuo kitos ir (arba) nuo fizinės aparatinės įrangos. Hipervizoriai gali veikti tiesiogiai aparatinėje įrangoje savarankiškai (angl. *bare metal*), operacinėje sistemoje arba kitoje virtualioje mašinoje (įdėtinė virtualizacija, angl. *nested virtualisation*). Šioje produktų kategorijoje virtualioji mašina yra programiškai nustatyta loginiu būdu atskirta kompiuterinė aplinka, apimanti virtualizuotų aparatinės įrangos išteklių rinkinį (pavyzdžiui, centrinį procesorių, atmintį, kaupiklį, tinklo sąsajas) ir paprastai turinti savo operacinę sistemą. Prie šios kategorijos, be kita ko, priskiriami 1 tipo (angl. *bare metal*), 2 tipo (veikiantys operacinėje sistemoje) ir mišrieji hipervizoriai.
	Konteinerių paleidimo sistemos yra tokie programinės įrangos produktai su skaitmeniniais elementais, kurie valdo konteinerių, vienoje pagrindinėje operacinėje sistemoje veikiančių kaip izoliuoti procesai, vykdymą ir gyvavimo ciklą, paskirsto išteklius ir sudaro galimybę valdyti ir suderinti pavienius konteinerius. Šioje produktų kategorijoje konteineris – programine įranga pagrįsta vykdymo aplinka, sudaryta iš vieno arba daugiau programinės įrangos komponentų ir jų tarpusavio priklausomybės ryšių viename pakete, todėl konteineris gali veikti nepriklausomai ir nuosekliai.
2. Užkardos, įsibrovimo aptikimo ir prevencijos sistemos	Užkardos yra produktai su skaitmeniniais elementais, kurie prijungtą tinklą arba sistemą nuo neleistinos prieigos saugo stebėdami ir ribodami duomenų perdavimo srautą į tą tinklą ir iš jo. Prie šios kategorijos, be kita ko, priskiriamos tinklo užkardos ir taikomųjų programų užkardos, pavyzdžiui, internetinių taikomųjų programų užkardos arba filtrai ir nuo brukalų apsaugantys sietuvai.
	Įsibrovimo aptikimo sistemos yra produktai su skaitmeniniais elementais, kurie stebėdami į tinklo aplinką atėjusį srautą ieško įtartino veikimo požymių ir aptinka arba atpažįsta bandymą įsibrauti, brovimąsi arba įsibrovimą į prijungtą tinklą arba sistemą. Prie šios kategorijos, be kita ko, priskiriamos tinkluose veikiančios įsibrovimo aptikimo sistemos ir serveriuose veikiančios įsibrovimo aptikimo sistemos.
	Įsibrovimo prevencijos sistemos yra produktai su skaitmeniniais elementais, kuriuos sudaro įsibrovimo aptikimo sistema, aktyviai reaguojanti į brovimąsi į prijungtą tinklą arba sistemą. Prie šios kategorijos, be kita ko, priskiriamos tinkluose veikiančios įsibrovimo prevencijos sistemos ir serveriuose veikiančios įsibrovimo prevencijos sistemos.

Produktų kategorija	Techninis aprašas
3. Klastojimui atsparūs mikroprocesoriai	Produktai su skaitmeniniais elementais, kurie yra šio priedo I klasės 13 punkte nurodyti mikroprocesoriai, kurie turi su saugumu susijusių funkcijų, įskaitant pažeidimo nustatymą, atsparumą arba reagavimą, ir kurie, be to, sukurti taip, kad užtikrina AVA_VAN 2 arba 3 lygio apsaugą, kaip nustatyta bendruosiuose kriterijuose ir bendrojoje vertinimo metodikoje.
4. Klastojimui atsparūs mikrovaldikliai	Produktai su skaitmeniniais elementais, kurie yra šio priedo I klasės 14 punkte nurodyti mikrovaldikliai, kurie turi su saugumu susijusių funkcijų, įskaitant pažeidimo nustatymą, atsparumą arba reagavimą, ir kurie, be to, sukurti taip, kad užtikrina AVA_VAN 2 arba 3 lygio apsaugą, kaip nustatyta bendruosiuose kriterijuose ir bendrojoje vertinimo metodikoje.

II PRIEDAS

YPATINGOS SVARBOS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS

Produktų kategorija	Techninis aprašas
1. Aparatinės įrangos prietaisai su seifais	Aparatinės įrangos produktai su skaitmeniniais elementais, kuriuose saugiai laikomi, apdorojami arba valdomi neskelbtini duomenys ir kurie sudaryti iš daugybės diskrečiųjų elementų; tokie produktai taip pat turi aparatinį fizinį gaubtą, būtiną pažeidimo nustatymui, atsparumui arba reagavimui kaip atsakomosioms priemonėms nuo fizinio brovimosi. Prie šios kategorijos, be kita ko, priskiriami fiziniai mokėjimo terminalai, aparatiniai saugumo moduliai, kuriais generuojami ir valdomi šifravimo elementai, ir pirmiau pateiktą aprašą atitinkantys tachografai.
2. Išmaniųjų skaitiklių tinklų sietuvai, naudojami pažangiosiose matavimo sistemose, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 ([1]) 2 straipsnio 23 punkte, ir kiti pažangieji saugumo prietaisai, be kita ko, skirti saugiam kriptografiniam apdorojimui	Išmaniųjų skaitiklių tinklų sietuvai – produktai su skaitmeniniais elementais, kuriais valdomas ryšys tarp komponentų, esančių Direktyvos (ES) 2019/944 2 straipsnio 23 punkte apibrėžtose pažangiosiose matavimo sistemose arba prijungtų prie tokių sistemų, ir įgaliotų trečiųjų šalių, pavyzdžiui, komunalinių paslaugų įmonių. Išmaniųjų skaitiklių tinklų sietuvai renka, apdoroja ir laiko skaitiklių ir asmens duomenis, apsaugo duomenis ir informacijos srautus, nes yra pritaikyti konkretiems šifravimo poreikiams, pavyzdžiui, duomenų užšifravimui ir iššifravimui, turi užkardos funkcijas ir suteikia priemones valdyti kitiems įrenginiams. Prie šios kategorijos, be kita ko, priskiriami išmaniųjų skaitiklių tinklų sietuvai, susiję su Direktyvos (ES) 2019/944 2 straipsnio 23 punkte apibrėžtomis pažangiosiomis matavimo sistemomis, kuriomis matuojamas elektros energijos suvartojimas. Prie jos taip pat priskiriami išmaniųjų skaitiklių tinklų sietuvai, naudojami kitose pažangiosiose matavimo sistemose, kuriomis matuojamas kitų išteklių, pavyzdžiui, dujų arba šilumos, suvartojimas, jei toks sietuvas atitinka šį aprašą.
3. Išmaniosios kortelės arba panašūs prietaisai, įskaitant saugiuosius elementus	Saugieji elementai – mikrovaldikliai arba mikroprocesoriai, turintys su saugumu susijusių funkcijų, įskaitant pažeidimo nustatymą, atsparumą arba reagavimą. Juose paprastai laikomi, apdorojami arba valdomi šifravimo operacijų arba neskelbtini duomenys, pavyzdžiui, tapatybės kredencialai arba mokėjimo kredencialai. Saugieji elementai sukurti taip, kad užtikrintų bent AVA_VAN 4 lygio apsaugą, kaip nustatyta bendruosiuose kriterijuose ir bendrojoje vertinimo metodikoje. Jie gali būti atskiruose silicio lustuose arba integruoti į vienalustes sistemas (angl. *systems on chip*, SoC). Saugiuosiuose elementuose gali būti taikomoji aplinka arba operacinė sistema, taip pat gali būti viena arba daugiau taikomųjų programų. Prie šios kategorijos, be kita ko, priskiriami patikimos platformos moduliai (angl. *trusted platform modules*, TPM) ir integruotos universalios lustinės kortelės (angl. *universal integrated circuit cards*, UICC).
	Išmaniosios kortelės arba panašios priemonės yra į kortelės formos bazinę medžiagą, pavyzdžiui, plastiką arba medieną, integruoti saugieji elementai arba į kitokios formos bazines medžiagas integruoti saugieji elementai. Prie šios kategorijos, be kita ko, priskiriami tapatybės ir kelionės dokumentai, kvalifikuoto parašo kortelės, pakeičiamosios UICC, fizinės mokėjimo kortelės, fizinės prieigos kortelės, skaitmeninio tachografo kortelės arba apyrankės su integruotais saugiaisiais mokėjimo elementais.

([1]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/944 dėl elektros energijos vidaus rinkos bendrųjų taisyklių, kuria iš dalies keičiama Direktyva 2012/27/ES, (OL L 158, 2019 6 14, p. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).