Europos Sąjungos
oficialusis leidinys

LT
C serija

C/2026/6013

2026 11 17

KOMISIJOS KOMUNIKATAS

Komisijos gairės dėl Reglamento (ES) 2024/2847 (Kibernetinio atsparumo akto) taikymo

(C/2026/6013)

Turinys

Puslapis

1. ĮVADAS ... 3
   1.1. Kibernetinio atsparumo aktas ... 3
   1.2. Gairių tikslas ... 3
2. TAIKYMO SRITIS ... 4
   2.1. Pateikimas rinkai ... 4
   2.2. Programinė įranga kaip produktas su skaitmeniniais elementais ... 5
   2.3. Kompiuterinis kodas ... 6
   2.4. Aparatinės ir programinės įrangos derinys, sudarantis produktą su skaitmeniniais elementais ... 7
   2.5. Duomenų jungtis ... 8
   2.6. Sudėtingos sistemos ... 8
   2.7. Produktai su skaitmeniniais elementais, suprojektuoti iki KAA taikymo pradžios ... 9
3. LAISVOJI IR ATVIROJI PROGRAMINĖ ĮRANGA ... 11
   3.1. Nustatymas, ar už laisvąją ir atvirąją programinę įrangą atsako konkretus asmuo ... 12
   3.2. Nustatymas, ar laisvoji ir atviroji programinė įranga pateikiama ES rinkai ... 13
      3.2.1. Mokesčio nustatymas ... 13
      3.2.2. Kitų paslaugų monetizavimas arba poreikis tvarkyti asmens duomenis ... 13
      3.2.3. Palaikymo paslaugos ... 14
      3.2.4. Aukos ... 15
      3.2.5. Laisvosios ir atvirosios programinės įrangos finansavimas ... 15
      3.2.6. Ne pelno tikslais įsteigti pelno nesiekiantys subjektai ... 16
      3.2.7. Integravimas, kurį atlieka kiti gamintojai ... 16
   3.3. Atvirosios programinės įrangos valdytojai ... 16
      3.3.1. Nuolatinė parama ir FOSS gyvybingumo užtikrinimas ... 17
   3.4. Prisidedantys asmenys ir tolesni naudojimo būdai ... 18
   3.5. Iliustraciniai scenarijai ... 19
4. ESMINIAI PAKEITIMAI IR ATSARGINĖS DALYS ... 21
   4.1. Fizinis taisymas ... 22
   4.2. Atsarginės dalys ... 23
   4.3. Programinės įrangos naujinimai kaip esminiai pakeitimai ... 24

4.4. Esminio pakeitimo pasekmės 27
4.4.1. Esminiai pakeitimai, kuriuos atlieka kitas nei pirminis gamintojas asmuo 28
4.4.2. Esminiai pakeitimai, kuriuos atlieka pirminis gamintojas 29
5. PALAIKYMO LAIKOTARPIS 29
5.1. Esminiai pakeitimai ir palaikymo laikotarpis 31
6. SVARBŪS IR YPATINGOS SVARBOS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS 32
6.1. Pagrindinė funkcija 33
6.2. Svarbių ir ypatingos svarbos produktų su skaitmeniniais elementais atitikties vertinimas 36
6.3. Atitikties prezumpcijos aspektai 38
7. KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS IR PRODUKTŲ SU SKAITMENINIAIS ELEMENTAIS BEI KOMPONENTŲ INTEGRAVIMAS 41
7.1. Kibernetinio saugumo rizikos vertinimas ir valdymas 41
7.2. Produktų su skaitmeniniais elementais projektavimas, kūrimas ir gamyba užtikrinant riziką atitinkantį jų kibernetinio saugumo lygį 42
7.3. Rizikos vertinimas ir išsamus patikrinimas, susiję su išorine priklausomybe ir integruotais komponentais 42
7.4. Rizikos vertinimų ir atitikties dokumentų pakartotinis naudojimas produktų su skaitmeniniais elementais grupėms 44
8. NUOTOLINIS DUOMENŲ TVARKYMAS 44
8.1. Kas laikoma produkto su skaitmeniniais elementais nuotolinio duomenų tvarkymo sprendiniu? 45
8.1.1. Sąvoka „per atstumą“ 46
8.1.2. Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų? 46
8.1.3. Ar programinę įrangą projektavo ir kūrė gamintojas arba tai buvo daroma jo atsakomybe? 47
8.2. Nuotolinio duomenų tvarkymo sprendinių ir kliovimosi trečiųjų šalių sprendiniais praktinės ir techninės pasekmės 49
8.3. Nuotolinio duomenų tvarkymo sprendinių naudojimo atvejai 50
8.3.1. Mobiliosios bankininkystės programėlė 51
8.3.2. Išmanusis termostatas 52
8.3.3. Elektroninių knygų skaityklė 53
8.3.4. Pramoninis robotas 53
8.3.5. Korinio ryšio tinklas 53
9. PAPILDOMI ELEMENTAI 54
9.1. Pareigos pranešti 54
9.2. Pažeidžiamumo valdymas 56
9.2.1. Pranešimų teikimas pirmesnės tiekimo grandies subjektams ir dalijimasis saugumo pataisomis . 56
9.2.2. Žinomas pažeidžiamumas, kuris gali būti išnaudojamas 57
9.2.3. Veiksmingi ir reguliarūs bandymai ir peržiūros 58
9.3. Sąveika su kitais teisės aktais 59
9.3.1. Reglamentas (ES) 2019/2144 ir Reglamentas (ES) Nr. 168/2013 59
9.3.2. ES tipo tyrimo sertifikatų galiojimas (69 straipsnio 1 dalis) 59

1. ĮVADAS

1.1. Kibernetinio atsparumo aktas

1. 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (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]) įsigaliojo 2024 m. gruodžio 10 d. Šiuo reglamentu siekiama sustiprinti ES požiūrį į kibernetinį saugumą, spręsti kibernetinio atsparumo klausimus ES lygmeniu ir gerinti vidaus rinkos veikimą, nustatant vienodą teisinę sistemą, kurioje įtvirtinami esminiai kibernetinio saugumo reikalavimai, taikomi produktų su skaitmeniniais elementais pateikimui ES rinkai, taip pat per visą produkto su skaitmeniniais elementais gyvavimo ciklą.

2. Kibernetinio atsparumo aktas (toliau – KAA) grindžiamas ES naująja teisės aktų sistema (NTAS), nustatyta 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008, nustatančiu su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinančiu Reglamentą (EEB) Nr. 339/93, ir 2008 m. liepos 9 d. Europos Parlamento ir Tarybos sprendimu Nr. 768/2008/EB dėl bendrosios gaminių pardavimo sistemos ir panaikinančiu Sprendimą 93/465/EEB ([2]).

3. Rinkos priežiūrą atlieka ir reikalavimų vykdymą užtikrina nacionalinės rinkos priežiūros institucijos. Produktams su skaitmeniniais elementais, patenkantiems į KAA taikymo sritį, taikomas 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1020 dėl rinkos priežiūros ir gaminių atitikties, kuriuo iš dalies keičiama Direktyva 2004/42/EB ir reglamentai (EB) Nr. 765/2008 ir (ES) Nr. 305/2011. Ekonominės veiklos vykdytojams ir valstybėms narėms taikyti KAA padeda Komisija ir Europos Sąjungos kibernetinio saugumo agentūra (ENISA).

1.2. Gairių tikslas

4. Pagal KAA 26 straipsnio 1 dalį Komisija privalo paskelbti gaires, skirtas padėti ekonominės veiklos vykdytojams taikyti šį reglamentą, ypatingą dėmesį skiriant tam, kad labai mažoms, mažosioms ir vidutinėms įmonėms (MVĮ) būtų lengviau laikytis reikalavimų. 26 straipsnio 2 dalyje nustatyti būtiniausi aspektai, kurie turėtų būti aptarti gairėse. Tarp jų yra: i) KAA taikymo sritis (visų pirma nuotolinio duomenų tvarkymo sprendiniai ir laisvoji bei atviroji programinė įranga); ii) sąvoka „palaikymo laikotarpiai“; iii) KAA ir kitų ES teisės aktų tarpusavio sąveika; iv) esminio pakeitimo samprata.

5. 2025 m. gruodžio 3 d. Komisija paskelbė atsakymus į dažnai užduodamus klausimus (DUK), skirtus padėti ekonominės veiklos vykdytojams pasirengti KAA įgyvendinimui ([3]).

6. Šiomis gairėmis siekiama padėti ekonominės veiklos vykdytojams laikytis KAA, o rinkos priežiūros institucijoms, notifikuojančiosioms institucijoms ir notifikuotosioms įstaigoms – vykdyti savo veiklą, kad visoje Sąjungoje būtų užtikrintas suderintas KAA vykdymas. Šiomis gairėmis nesiekiama išsamiai aprėpti visos KAA taikymo srities; jomis siekiama paaiškinti tam tikrų pagrindinių nuostatų loginį pagrindą ir tai, kaip jos galėtų būti įgyvendinamos praktiškai. Šios gairės yra susijusios su KAA ir netaikomos kitiems ES teisės aktams.

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

([2]) Komisijos 2026 m. darbo programoje numatyta pateikti Europos gaminių aktą, kuriuo atnaujinama NTAS ir rinkos priežiūros bei standartizacijos taisyklės (https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52025DC0870).

([3]) DUK galima parsisiųsti iš Komisijos KAA įgyvendinimo svetainės specialaus DUK tinklalapio.

7. Rengiant šias gaires buvo išsamiai konsultuojamasi su suinteresuotaisiais subjektais, be kita ko, Produktų su skaitmeniniais elementais kibernetinio saugumo ekspertų grupėje ([4]), taip pat per viešas konsultacijas, surengtas 2026 m. kovo 3 d. – balandžio 13 d ([5]).

8. Šios gairės nėra privalomos ekonominės veiklos vykdytojams ar kitiems subjektams, kuriems taikomas KAA. Autoritetingą KAA aiškinimą gali pateikti tik Europos Sąjungos Teisingumo Teismas. Vis dėlto šiose gairėse išdėstomas Komisijos pateikiamas KAA aiškinimas, siekiant padėti laikytis to reglamento reikalavimų ir prisidėti prie veiksmingo jo įgyvendinimo. Be to, gairėse pateikiama pavyzdžių, kuriais iliustruojamas konkrečių nuostatų taikymas, tačiau šie pavyzdžiai neatstoja kiekvieno atvejo individualaus vertinimo, kuris visada bus reikalingas siekiant atsižvelgti į kiekvieno atskiro atvejo specifiką.

9. Pagal KAA 26 straipsnį, Komisija gali apsvarstyti galimybę paskelbti papildomas gaires, įskaitant gaires, skirtas gamintojams, kuriems taikomas KAA ir kiti Sąjungos derinamieji teisės aktai arba kiti susiję Sąjungos teisės aktai. Tokiose gairėse, pavyzdžiui, galėtų būti nagrinėjami klausimai, susiję su sąveika tarp KAA ir Reglamento (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės, (DI akto) bei Reglamento (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje (SVAA).

2. **TAIKYMO SRITIS**

2.1. **Pateikimas rinkai**

10. KAA taikomas ES rinkai tiekiamiems produktams su skaitmeniniais elementais. Tiekimo rinkai sąvoka KAA 3 straipsnio 22 punkte apibrėžiama kaip „produkto su skaitmeniniais elementais tiekimas platinti ar naudoti Sąjungos rinkoje vykdant komercinę veiklą už atlygį arba nemokamai“. Pagal 3 straipsnio 21 punktą, produktas su skaitmeniniais elementais pateikiamas ES rinkai tada, kai jis tai rinkai tiekiamas pirmą kartą.

11. Naujausiame 2022 m. paskelbtame Mėlynajame vadove dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo (toliau – Mėlynasis vadovas) ([6]) pateikiamos gairės, padedančios suprasti gaminius reglamentuojančias ES taisykles ir vienodai jas taikyti įvairiose sektorių teisinėse sistemose, suderintose su naująja teisės aktų sistema (NTAS), kaip antai KAA. Mėlynajame vadove nurodoma, kad sąvokos „pateikimas rinkai“ ir „tiekimas rinkai“ turi būti suprantamos kaip vartojamos turint omenyje „kiekvieną atskirą gaminį, o ne gaminio rūšį ir tai, ar jis pagamintas vienetinės, ar serijinės gamybos būdu“ (2.3 skirsnis).

12. Kalbant apie įprastesnius produktus su skaitmeniniais elementais, kuriems taikoma NTAS, pavyzdžiui, aparatinę įrangą – mašinų ar radijo įrenginių pavidalo produktus su skaitmeniniais elementais, – „pateikimo rinkai“ sąvoka yra nusistovėjusi, o Mėlynajame vadove pateikiamos papildomos gairės, kuriose paaiškinama, kada tokie produktai laikomi pateiktais rinkai. Mėlynojo vadovo 2.12 skirsnyje „Apibendrinamieji pavyzdžiai“ pateikiama daugiau sąvokos „pateikimas rinkai“ vartosenos pavyzdžių.

13. Tačiau, atsižvelgiant į nematerialių produktų su skaitmeniniais elementais, pavyzdžiui, autonominės programinės įrangos, pobūdį, reikia papildomų gairių dėl to, kada tokie produktai su skaitmeniniais elementais laikomi pateiktais rinkai. Kai užbaigiamas programinės įrangos gamybos etapas ir produktas su skaitmeniniais elementais pasiūlomas potencialiems naudotojams ES rinkoje, galima laikyti, kad jo gamintojas pagamino kelias to paties programinės įrangos produkto su skaitmeniniais elementais kopijas ir patiekė jas platinti arba naudoti. Iš tiesų, kitaip nei materialiems produktams su skaitmeniniais elementais, autonominei programinei įrangai netaikomi

([4]) Produktų su skaitmeniniais elementais kibernetinio saugumo ekspertų grupė Komisijos ekspertų grupių ir kitų panašių subjektų registre.
([5]) Viešos konsultacijos dėl Komisijos Kibernetinio atsparumo akto taikymo gairių projekto.
([6]) Komisijos pranešimas „2022 m. Mėlynasis vadovas dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo“, 2022/C 247/01 (OL C 247, 2022 6 29, p. 1).

fizinės gamybos ar atsargų apribojimai: kiekvieną kartą programinę įrangą padarius prieinamą parsisiųsti ar platinti naudotojui, sukuriama nauja identiška jos kopija. Kol ši programinės įrangos versija nėra pakeista taip, kad tai turėtų įtakos atitikčiai KAA, laikoma, kad ji pateikta ES rinkai tuo momentu, kai pirmą kartą pasiūloma ją platinti arba naudoti. Todėl galimybė vėliau parsisiųsti ar platinti šią programinės įrangos produkto su skaitmeniniais elementais versiją laikytina šio programinės įrangos produkto su skaitmeniniais elementais tiekimu rinkai ([7]).

14. Todėl autonominis programinės įrangos produktas su skaitmeniniais elementais turėtų būti laikomas pateiktu rinkai tada, kai užbaigiamas jo gamybos etapas ir ši programinė įranga pirmą kartą tiekiama platinti arba naudoti ES rinkoje vykdant komercinę veiklą. Turėtų būti laikoma, kad gamintojas tuo pačiu metu pateikė rinkai kelias to paties programinės įrangos produkto su skaitmeniniais elementais kopijas. Todėl, nors kelios tos pačios programinės įrangos kopijos tebėra atskiri produktai su skaitmeniniais elementais, laikoma, kad jos pateiktos rinkai tuo pačiu metu, neatsižvelgiant į tai, kada kiekvienos atskiros kopijos nuosavybė ar naudojimas perleidžiami kitam fiziniam ar juridiniam asmeniui. Tačiau, kai gamintojas tiekia skirtingus programinės įrangos variantus, kurie skiriasi į juos įtrauktais komponentais, konfigūracijomis ar įdiegtomis funkcijomis, pavyzdžiui, skirtingoms operacinėms sistemoms skirtas versijas arba paketus su skirtingais funkcijų rinkiniais, tokie variantai negali būti laikomi keliomis to paties programinės įrangos produkto su skaitmeniniais elementais kopijomis. Todėl pateikimo rinkai tikslais jie turėtų būti laikomi atskirais produktais su skaitmeniniais elementais.

1 pavyzdys. 2028 m. sausio 1 d. įmonė A savo svetainėje pirmą kartą tiekia platinti savo X programinės įrangos 1.0.0 versiją. Tą pačią dieną 1-asis klientas įsigyja X programinės įrangos 1.0.0 versijos kopiją. 2028 m. sausio 15 d. 2-asis klientas įsigyja X programinės įrangos 1.0.0 versijos kopiją. Laikoma, kad abi X programinės įrangos 1.0.0 versijos kopijos pateiktos rinkai 2028 m. sausio 1 d.

15. Atsižvelgiant į iteracinį (kartotinį) programinės įrangos kūrimo pobūdį, taip pat reikėtų paaiškinti, kad programinės įrangos produkto su skaitmeniniais elementais vėlesnės versijos laikomos naujai pateiktomis rinkai, kai tokias versijas tinka laikyti jau rinkai pateikto programinės įrangos produkto su skaitmeniniais elementais „esminiu pakeitimu“, kaip nurodyta KAA 41 konstatuojamojoje dalyje. Vėlesnių versijų, kurios nelaikytinos esminiais pakeitimais, atveju gamintojas neprivalo atlikti naujos atitikties vertinimo procedūros, todėl tos programinės įrangos pateikimo rinkai data nekeičiama. Daugiau gairių dėl esminių pakeitimų sampratos pateikiama 4 skirsnyje „*Esminiai pakeitimai*“.

2 pavyzdys. 2028 m. sausio 1 d. įmonė A savo svetainėje pirmą kartą tiekia platinti X programinės įrangos 1.0.0 versiją. Tą pačią dieną 1-asis klientas įsigyja X programinės įrangos 1.0.0 versijos kopiją. 2028 m. sausio 15 d. įmonė A išleidžia atnaujintą X programinės įrangos 1.0.1 versiją, kuri nėra esminis pakeitimas. 2028 m. sausio 30 d. 2-asis klientas įsigyja X programinės įrangos 1.0.1 versijos kopiją. Laikoma, kad tiek X programinės įrangos 1.0.0 versijos, tiek 1.0.1 versijos kopijos pateiktos rinkai 2028 m. sausio 1 d.

16. 13, 14 ir 15 punktuose išdėstytos gairės taikomos tik tiek, kiek produktas su skaitmeniniais elementais yra autonominė programinė įranga. Taip nėra, pavyzdžiui, tais atvejais, kai programinė įranga yra derinama su aparatine įranga, kaip aptariama 2.4 skirsnyje „*Aparatinės ir programinės įrangos derinys, sudarantis produktą*“.

2.2. **Programinė įranga kaip produktas su skaitmeniniais elementais**

17. KAA 3 straipsnio 1 punkte produktas su skaitmeniniais elementais apibrėžiamas kaip „programinės ar aparatinės įrangos produktas ir jo nuotolinio duomenų tvarkymo sprendiniai, įskaitant atskirai rinkai pateikiamus programinės ar aparatinės įrangos komponentus“. Tokie produktai su skaitmeniniais elementais patenka į KAA taikymo sritį, jeigu jų numatytoji paskirtis arba pagrįstai numatomas naudojimas apima tiesioginę arba netiesioginę loginę ar fizinę duomenų jungtį su įrenginiu arba tinklu.

([7]) Pagal 13 straipsnio 11 dalį, gamintojai gali laikyti viešus programinės įrangos archyvus, kad ankstesnės programinės įrangos versijos būtų lengviau prieinamos naudotojams. Tokiais atvejais naudotojai turi būti aiškiai ir lengvai prieinamu būdu informuojami apie riziką, susijusią su nebepalaikomos programinės įrangos naudojimu.

18. Todėl KAA gali būti taikomas įvairiems produktams su skaitmeniniais elementais, įskaitant: i) autonominę programinę įrangą, pavyzdžiui, mobiliąsias programėles ir kompiuterių programas, nepriklausomai nuo to, ar jos platinamos skaitmeniniu, ar fiziniu būdu; ii) aparatinę įrangą su įtaisytąja programine įranga (pvz., daiktų interneto prietaisus, nešiojamuosius kompiuterius, planšetinius kompiuterius); iii) autonominę aparatinę įrangą (pvz., integrinius grandynus, pagrindines plokštes) ir iv) bet kokį atskirai tiekiamos, bet kartu veikti skirtos aparatinės ir programinės įrangos derinį.

19. Taigi autonominė programinė įranga patenka į KAA taikymo sritį, jeigu ji pateikiama rinkai kaip produktas su skaitmeniniais elementais. Šiuo požiūriu naudinga skirti programinės įrangos produktus su skaitmeniniais elementais, kuriems taikomas KAA, nuo nuotoliniu būdu teikiamų paslaugų, kurios į KAA taikymo sritį nepatenka.

20. Kad programinei įrangai būtų taikomas KAA, programinės įrangos produktas su skaitmeniniais elementais turi būti pateiktas naudotojui, jo įgytas ir veikti naudotojo elektroninėje informacinėje sistemoje arba kaip jos dalis. Šiuos kriterijus atitinka programinė įranga, kuri parsisiunčiama, įdiegiama ar kitu būdu pateikiama naudotojui ir veikia jo elektroninėje informacinėje sistemoje, įskaitant, pavyzdžiui, naršyklės plėtinio pavidalo programinę įrangą arba naudojant saityno technologijas sukurtą taikomąją programą, kuri tiekiama vykdyti vietoje.

21. Kita vertus, vien šios aplinkybės nepakanka, kad programinė įranga, kurios programos vykdomos nuotoliniu būdu ir prie kurios naudotojas turi tik prieigą, būtų laikoma produktu su skaitmeniniais elementais. KAA 11 ir 12 konstatuojamosiose dalyse šis skirtumas aiškiai nustatomas paaiškinant, kad duomenų tvarkymui ar saugojimui per atstumą KAA taikomas tik tiek, kiek toks tvarkymas ar saugojimas yra būtinas, kad produktas su skaitmeniniais elementais galėtų atliktų savo funkcijas, (t. y. pagal 3 straipsnio 2 punkte apibrėžtą sąvoką „nuotolinis duomenų tvarkymas“), o ne kaip produktui su skaitmeniniais elementais. Paprastai taip yra saityno taikomųjų programų, įskaitant progresyviąsias internetines programėles, kai jos prieinamos tik per saityno naršyklę, atveju. Tas pats taikoma saityno svetainėms: nors techniniu požiūriu saityno svetainės ribotu mastu gali veikti ir būti vykdomos naudotojo įrenginyje, iš KAA 12 konstatuojamosios dalies matyti, kad pačios svetainės neturi būti laikomos produktais su skaitmeniniais elementais ir į KAA taikymo sritį patenka tik kai jos palaiko produkto su skaitmeniniais elementais funkcionalumą, t. y. tiek, kiek jų veikimas laikomas nuotoliniu duomenų tvarkymu (kaip išsamiau paaiškinta *8* skirsnyje, visų pirma *8.1.2 „Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų?“*).

3 pavyzdys. Mobilioji programėlė, kurią naudotojas parsisiunčia iš programėlių parduotuvės ir įdiegia savo išmaniajame telefone, yra tiekiama naudotojui ir vykdoma jo įrenginyje, todėl ji yra produktas su skaitmeniniais elementais. Jeigu ji pateikiama rinkai vykdant komercinę veiklą, ji gali patekti į KAA taikymo sritį.

4 pavyzdys. Naudojant saityno technologijas sukurta, tačiau vietiniam diegimui supakuota darbalaukio taikomoji programa yra tiekiama naudotojui ir vykdoma jo įrenginyje, todėl ji yra produktas su skaitmeniniais elementais. Jeigu ji pateikiama rinkai vykdant komercinę veiklą, ji gali patekti į KAA taikymo sritį.

5 pavyzdys. Saityno taikomoji programa, kuri naudotojui yra prieinama tik per saityno naršyklę, nėra produktas su skaitmeniniais elementais. Jeigu ji nepalaiko produkto su skaitmeniniais elementais funkcionalumo, ji nepatenka į KAA taikymo sritį. Kita vertus, naudotojui kaip vietoje įdiegiama kliento programa tiekiama taikomoji programa, kuri vykdoma naudotojo įrenginyje, yra produktas su skaitmeniniais elementais. Jeigu ji pateikiama rinkai vykdant komercinę veiklą, ji gali patekti į KAA taikymo sritį.

Jeigu tai kliento programai, kad ji galėtų atlikti vieną ar daugiau savo funkcijų, reikalingas duomenų tvarkymas per atstumą, atitinkantis nuotolinio duomenų tvarkymo apibrėžtį, toks duomenų tvarkymas per atstumą taip pat yra produkto su skaitmeniniais elementais dalis.

6 pavyzdys. Saityno svetainė, kurioje lankytojams tik pateikiama informacija ir kuri nepalaiko produkto su skaitmeniniais elementais funkcionalumo, pati nėra produktas su skaitmeniniais elementais, todėl ji nepatenka į KAA taikymo sritį.

2.3. **Kompiuterinis kodas**

22. Taip pat naudinga paaiškinti, ar pirminis kodas gali būti laikomas programinės įrangos produktu su skaitmeniniais elementais. KAA programinė įranga apibrėžiama kaip „elektroninės informacinės sistemos dalis, sudaryta iš kompiuterinio kodo“ (3 straipsnio 4 punktas). Kompiuterinis kodas gali būti i) mašininis kodas, t. y. dvejetainiu formatu užrašytų komandų, kurias tiesiogiai vykdo kompiuterio procesorius, rinkinys, arba ii) pirminis kodas, t. y. programavimo kalba užrašytų komandų ir teiginių rinkinys, kuris, kad galėtų būti vykdomas kompiuterio, turi būti kompiliuojamas arba interpretuojamas. KAA nustatyta programinės įrangos apibrėžtis apima abi šias formas.

23. Atskiras klausimas yra tai, ar konkretus kompiuterinio kodo tiekimas laikytinas produkto su skaitmeniniais elementais pateikimu ES rinkai, nes tam būtina sąlyga yra tiekimas vykdant komercinę veiklą. Pirminio kodo atveju dažnai gali taip nebūti. Pavyzdžiui, fizinis ar juridinis asmuo, kuris viešai prieinamose saugyklose dalijasi laisvuoju ir atviruoju kompiuteriniu kodu, paprastai nelaikomas pateikiančiu tokį kodą ES rinkai pagal KAA (kaip išsamiau aptarta 3 skirsnyje „*Laisvoji ir atviroji programinė* įranga“). Nebaigtas kodas, kuriuo dalijamasi produkto su skaitmeniniais elementais projektavimo ir kūrimo etape (pvz., bandymo ar peržiūros tikslais), taip pat nelaikomas pateiktu rinkai pagal KAA, nes jo gamybos etapas dar nėra užbaigtas. Panašiai ir pavyzdinis arba demonstracinis kodas, pateikiamas kaip mokomųjų leidinių ar mokymo medžiagos dalis, nelaikomas pateiktu rinkai pagal KAA ([8]).

24. Kita vertus, kai gamintojas kompiuterinį kodą pateikia savo klientams kaip produktą su skaitmeniniais elementais, laikoma, kad toks kodas yra pateiktas rinkai, neatsižvelgiant į tai, ar tai yra mašininis ar pirminis kodas ([9]).

7 pavyzdys. Įmonė A suteikia įmonei B licenciją naudoti pirminį kodą, skirtą pritaikomai vidaus platformai, ir šį pirminį kodą pateikia tekstiniame faile. Net jei prieš naudojant šį pirminį kodą įmonei B dar reikia jį pritaikyti ir sukompiliuoti, įmonė A šį pirminį kodą pateikia rinkai, todėl jai taikomas KAA. Įmonė A neatsako už įmonės B vėliau atlikto šio kodo pritaikymo ir kompiliavimo atitiktį KAA.

2.4. **Aparatinės ir programinės įrangos derinys, sudarantis produktą su skaitmeniniais elementais**

25. Ar programinė įranga yra produkto su skaitmeniniais elementais dalis, turėtų būti nustatoma ne pagal tai, kaip ar kada ši programinė įranga pateikiama naudotojui, o pagal tai, ar, atsižvelgiant į produkto numatytąją paskirtį ir pagrįstai numatomą naudojimą, programinė įranga yra būtina tam, kad produktas su skaitmeniniais elementais galėtų atlikti numatytąsias funkcijas. Kai aparatinės įrangos produktas su skaitmeniniais elementais yra suprojektuotas veikti kartu su konkrečia to paties gamintojo teikiama programine įranga tam, kad galėtų atlikti savo funkcijas, aparatinė ir programinė įranga kartu sudaro produktą su skaitmeniniais elementais. Todėl programinė įranga, kuri yra būtina produktui su skaitmeniniais elementais eksploatuoti, konfigūruoti, valdyti ar naudoti pagal jo numatytąją paskirtį, yra produkto su skaitmeniniais elementais dalis, net jeigu ji gaunama atskiru kanalu (pvz., iš programėlių parduotuvės, naudojantis parsisiuntimo nuoroda ar kitu skaitmeniniu kanalu po to, kai aparatinės įrangos produktas su skaitmeniniais elementais jau pateiktas rinkai). Todėl laikoma, kad tokia programinė įranga pateikiama rinkai tuo pačiu metu, kai rinkai pateikiami atitinkami aparatinės įrangos produktų su skaitmeniniais elementais vienetai.

8 pavyzdys. Tinklo spausdintuvas pateikiamas rinkai kaip aparatinės įrangos produktas su skaitmeniniais elementais, o programinės įrangos tvarkyklės, reikalingos spausdinimo užduotims siųsti, įrenginiui konfigūruoti ir jo veikimui valdyti, pateikiamos parsisiųsti iš gamintojo svetainės. Nors spausdintuvas ir tvarkyklės tiekiami skirtingais kanalais, kartu jie sudaro vieną produktą su skaitmeniniais elementais, nes be tvarkyklių spausdintuvas negali atlikti numatytosios paskirties.

9 pavyzdys. Dėvimasis kūno rengybos prietaisas pateikiamas rinkai naudotojo širdies ritmui ir fiziniam aktyvumui matuoti, o gamintojo teikiama išmaniojo telefono programėlė yra būtina matavimo rezultatams rodyti, ankstesniems duomenims peržiūrėti ir prietaisui konfigūruoti. Nors programėlė atskirai parsisiunčiama iš programėlių parduotuvės, dėvimasis prietaisas ir programėlė kartu sudaro vieną produktą su skaitmeniniais elementais, nes jie suprojektuoti ir skirti veikti kartu, kad būtų užtikrintas produkto su skaitmeniniais elementais funkcionalumas.

([8]) Taip pat reikėtų priminti, kad pagal 4 straipsnio 3 dalį gamintojams leidžiama tiekti rinkai reglamento neatitinkančią nebaigtą programinę įrangą, pavyzdžiui, alfa versijas, beta versijas arba kandidatines versijas, su sąlyga, kad nebaigta programinė įranga būtų prieinama tik tiek laiko, kiek būtina jai išbandyti ir grįžtamajai informacijai gauti.

([9]) Kita vertus, pažymėtina, kad atsakomybės už gaminius teisės aktų taikymo tikslais pats kompiuterinis kodas nelaikomas gaminiu, todėl gamintojai, pateikiantys tokį kodą rinkai, negali būti laikomi atsakingais pagal Direktyvą (ES) 2024/2853 (Atsakomybės už gaminius direktyvą). Tos direktyvos 13 konstatuojamojoje dalyje nurodyta, kad „[t]ačiau informacija neturi būti laikoma gaminiu, todėl atsakomybės už gaminį taisyklės neturėtų būti taikomos skaitmeninių rinkmenų turiniui, pavyzdžiui, medijos rinkmenoms ar e. knygoms arba programinės įrangos pirminiam kodui“. Tai neužkerta kelio gamintojų atsakomybei pagal nacionalinę deliktų teisę.

2.5. **Duomenų jungtis**

26. 2 straipsnio 1 dalyje nustatyta, kad KAA „taikomas rinkai patiektiems produktams su skaitmeniniais elementais, kurių numatytoji paskirtis arba pagrįstai numatomas naudojimas apima tiesioginę arba netiesioginę loginę arba fizinę duomenų jungtį su įrenginiu arba tinklu“. Taigi KAA taikymo sritis grindžiama ne vien elektronikos komponentų buvimu produkte, bet ir produkto su skaitmeniniais elementais gebėjimu keistis skaitmenine informacija.

27. Nors sąvokos „loginė jungtis“ ir „fizinė jungtis“ apibrėžtos 3 straipsnyje, sąvokos „duomenų jungtis“ ir „skaitmeniniai duomenys“ KAA neapibrėžtos. Todėl, siekiant aiškiau nustatyti KAA taikymo srities ribas, naudinga paaiškinti, kaip turėtų būti suprantama duomenų jungtis. Šios ribos yra ypač svarbios siekiant skirti produktus su skaitmeniniais elementais, kuriuose tik naudojami elektriniai signalai, nuo produktų, kurie naudojami skaitmeninėje komunikacijoje ir dėl to jiems kyla kibernetinio saugumo rizika.

28. Paprasčiausio lygmens duomenų jungtis apima informacijos perdavimą dvejetaine forma, t. y. kaip nulių ir vienetų seką. Vien išvesties signalo įjungimas ir išjungimas (t. y. 0/1) savaime nėra duomenų jungtis, jeigu šios būsenos nėra skirtos duomenims išreikšti arba jų nenuskaito skaitmeninė įvestis. Kad egzistuotų duomenų jungtis, dvejetainės būsenos šaltinyje turi būti sąmoningai užkoduotos kaip informacija, o paskirties vietoje turi būti įmanoma jas iškoduoti kaip informaciją. Kitaip tariant, turi būti siuntėjas, kuris pagal nustatytą schemą sąmoningai generuoja skaitmeninius simbolius, ir imtuvas, galintis tuos simbolius interpretuoti kaip duomenis. Kai elektriniai ar elektroniniai signalai naudojami tik funkcijai suaktyvinti arba energijai jai tiekti, tačiau jais neperduodama skaitmeniniu būdu užkoduota informacija, KAA taikymo tikslais duomenų jungties nėra, todėl toks produktas su skaitmeniniais elementais nepatenka į 2 straipsnio 1 dalies taikymo sritį.

2.6. **Sudėtingos sistemos**

29. Į KAA taikymo sritį patenkantys produktai su skaitmeniniais elementais gali būti ne tik pavieniai įrenginiai ar programinės įrangos komponentai, bet ir sudėtingos sistemos, įskaitant sistemas, sudarytas iš kelių aparatinės ir programinės įrangos elementų, kurie veikia kartu atlikdami tam tikrą funkciją. Kai tokia sistema pateikiama rinkai kaip vienas produktas su skaitmeniniais elementais, ji laikoma produktu su skaitmeniniais elementais, kaip tai suprantama pagal KAA.

30. Tokioms sudėtingoms sistemoms dažnai būdingi ilgi projektavimo ir kūrimo ciklai, sutartys, kurios galėjo būti sudarytos dar iki KAA taikymo pradžios, ilgas eksploatavimo laikotarpis ir didelis techninis bei organizacinis sudėtingumas. Tokiose sistemose, kurios rinkai pateikiamos jau pradėjus taikyti KAA, gali būti naudojami komponentai, pateikti rinkai iki KAA taikymo pradžios, jų architektūra gali būti nusistovėjusi arba jose gali būti plačiai naudojami sąveikumo standartai, įskaitant kituose ES teisės aktuose ar konkretiems sektoriams skirtose sistemose nurodytus standartus. Todėl tam tikras tokių sistemų techninės charakteristikas gali būti sunku arba neproporcinga keisti nedarant poveikio jų numatytajai paskirčiai, saugai, patikimumui ar sąveikumui su esama infrastruktūra.

31. Šios charakteristikos savaime nereiškia, kad sudėtingos sistemos nepatenka į KAA taikymo sritį. Veikiau jos parodo, kaip taikomas KAA rizika grindžiamas požiūris, pagal kurį, vadovaujantis KAA 13 straipsnio 3 dalimi, atitiktis gali būti įrodoma įvairiais būdais, atsižvelgiant į produkto su skaitmeniniais elementais charakteristikas ir apribojimus. Šios charakteristikos yra produkto numatytosios paskirties ir jo eksploatavimo aplinkybių dalis, todėl yra svarbios vertinant atitiktį esminiams kibernetinio saugumo reikalavimams (toliau – esminiai reikalavimai). Visų pirma 55 konstatuojamojoje dalyje aiškiai pripažįstama, kad tam tikri esminiai reikalavimai gali būti nevisiškai suderinami su produkto su skaitmeniniais elementais pobūdžiu. Pavyzdžiui, taip gali būti tuo atveju, kai reikalavimų laikymasis pakenktų privalomų sąveikumo reikalavimų laikymuisi arba tinkamam sistemos veikimui.

32. Atitinkamai gamintojai privalo spręsti kibernetinio saugumo rizikos klausimus remdamiesi 13 straipsnio 2 dalyje nurodytu kibernetinio saugumo rizikos vertinimu. Kaip paaiškinta ir 55 konstatuojamojoje dalyje, tam tikrais atvejais konkretūs esminiai reikalavimai netaikomi arba jų neįmanoma įvykdyti taikant pažangiausias saugumo

priemones, pavyzdžiui, dėl sistemos numatytosios paskirties, dėl kurios produktas su skaitmeniniais elementais turi sąveikauti su esamais priklausomybės šaltiniais arba atitikti tam tikrus sąveikumo reikalavimus. Tokiais atvejais gamintojai turėtų nustatyti ir dokumentuoti tokius konkrečius apribojimus, įvertinti su jais susijusią riziką ir įgyvendinti tinkamas alternatyvias arba kompensacines rizikos mažinimo priemones, kad nebūtų pakenkta produkto su skaitmeniniais elementais saugumui. Šiuo tikslu svarbus vaidmuo tenka tiek 31 straipsnyje nurodytiems techniniams dokumentams, tiek II priede nurodytai naudotojui teikiamai informacijai ir instrukcijoms, nes juose skaidriai aprašomi nustatyti apribojimai, su jais susijusi kibernetinio saugumo rizika ir įgyvendintos rizikos mažinimo priemonės. Atlikdami pareigą palaikymo laikotarpiu nuolat atnaujinti rizikos vertinimą, gamintojai taip pat turėtų periodiškai iš naujo įvertinti, ar tokie apribojimai tebeegzistuoja. Jeigu laikui bėgant tokius apribojimus galima panaikinti arba sumažinti, gamintojai produktą su skaitmeniniais elementais turėtų atitinkamai atnaujinti, kad būtų galima laipsniškai pasiekti tinkamą kibernetinio saugumo lygį ([10]).

10 pavyzdys. Gamintojas pateikia rinkai produktą su skaitmeniniais elementais, kuris su išorinėmis sistemomis palaiko ryšį naudodamas tinklo protokolą. Taikydamas esminius reikalavimus, gamintojas, remdamasis kibernetinio saugumo rizikos vertinimu, nustato, kad duomenų, kuriais keičiamasi naudojant produktą su skaitmeniniais elementais, konfidencialumui ir vientisumui užtikrinti būtina naudoti saugų ryšio protokolą.

Tačiau produktas pagal numatytąją paskirtį turi būti sąveikus su esamomis sistemomis, kurios palaiko tik senesnį arba mažiau saugų protokolą. Tokiais atvejais gamintojas gali įdiegti tokį protokolą, jeigu tai būtina sąveikumui užtikrinti, su sąlyga, kad su tuo susijusi kibernetinio saugumo rizika būtų nustatyta ir mažinama kitomis priemonėmis.

Jeigu techniškai įmanoma, kad produktas su skaitmeniniais elementais palaikytų ir saugų, ir mažiau saugų protokolą, iš gamintojo tikimasi, kad jis įdiegs saugų protokolą ir nustatys, kad jis būtų taikomas pagal numatytąją parinktį. Mažiau saugų protokolą būtų leidžiama naudoti tik tais atvejais, kai tai būtina sąveikumui užtikrinti.

11 pavyzdys. Pramonės automatizavimo sistemos gamintojas iki KAA taikymo pradžios įsigyja tam tikrų mikrovaldiklių. Gamintojas atlieka savo pramonės automatizavimo sistemos, kuri bus pateikta rinkai pradėjus taikyti KAA, kibernetinio saugumo rizikos vertinimą. Remdamasis tuo kibernetinio saugumo rizikos vertinimu, gamintojas nenustato konkrečios kibernetinio saugumo rizikos, susijusios su vieno iš tų mikrovaldiklių naudojimu. Gamintojas integruoja jį į savo pramonės automatizavimo sistemą ir užtikrina, kad visas produktas su skaitmeniniais elementais (pramonės automatizavimo sistema) atitiktų esminius reikalavimus.

2.7. **Produktai su skaitmeniniais elementais, suprojektuoti iki KAA taikymo pradžios**

33. Kai kuriais atvejais gamintojas, 2027 m. gruodžio 11 d. pradėjus taikyti KAA, pateiks rinkai produkto su skaitmeniniais elementais vienetus, pagamintus pagal tipą ar modelį, kuris buvo suprojektuotas ir sukurtas iki KAA taikymo pradžios datos. Tokiais atvejais atitiktis šiam reglamentui nebūtinai reiškia, kad tie produkto su skaitmeniniais elementais vienetai turi būti perprojektuoti. Gamintojas privalo atlikti kibernetinio saugumo rizikos vertinimą pagal KAA 13 straipsnio 2 dalį, kad, remdamasis produkto su skaitmeniniais elementais numatytąja paskirtimi ir pagrįstai numatomu naudojimu, nustatytų, kurie iš I priedo I dalyje nustatytų esminių reikalavimų taikomi tam produktui su skaitmeniniais elementais ir kaip šie reikalavimai įgyvendinami.

34. Jeigu rizikos vertinimo rezultatai rodo, kad produkte su skaitmeniniais elementais jau įdiegtos tinkamos ir veiksmingos saugumo priemonės, kuriomis mažinama atitinkama rizika, gamintojas, siekdamas įrodyti atitiktį KAA, gali remtis šiomis jau taikomomis priemonėmis. Pačiame KAA nenustatyta pareiga įdiegti naujų saugumo funkcijų ar perprojektuoti produktą su skaitmeniniais elementais, jeigu tai nėra būtina nustatytai rizikai mažinti.

([10]) Pažymėtina, kad šioje dalyje išdėstyti argumentai, kai tinkama, gali būti taikomi visiems į KAA taikymo sritį patenkantiems produktams su skaitmeniniais elementais, o ne vien sudėtingoms sistemoms.

35. Vis dėlto gamintojui ir toliau taikomos KAA nustatytos pareigos. Be kita ko, prieš pateikdamas produktą su skaitmeniniais elementais rinkai, gamintojas turi užtikrinti, kad būtų atlikta taikytina atitikties vertinimo procedūra, parengta ES atitikties deklaracija ir produktas paženklintas CE ženklu. Šių reikalavimų laikymasis nepriklauso nuo to, ar, atsižvelgiant į rizikos vertinimo rezultatus, reikėjo pakeisti produkto su skaitmeniniais elementais projektą. Produktų su skaitmeniniais elementais, kurie buvo suprojektuoti iki KAA taikymo pradžios datos, tačiau rinkai pateikiami po šios datos, atveju, kai gamintojas negali parodyti, kaip į rizikos vertinimą buvo atsižvelgta produkto su skaitmeniniais elementais projektavimo ir kūrimo etape, 13 straipsnio 2 dalyje nustatyta pareiga turėtų būti suprantama kaip reikalavimas, kad gamintojai atliktų kibernetinio saugumo rizikos vertinimą ir jo pagrindu įrodytų, kad produkte su skaitmeniniais elementais įdiegtos tinkamos saugumo priemonės, kuriomis siekiama kuo labiau sumažinti kibernetinio saugumo riziką, užkirsti kelią incidentams ir kuo labiau sumažinti jų poveikį, be kita ko, naudotojų sveikatai ir saugai.

36. Atitinkamai produktai su skaitmeniniais elementais, suprojektuoti iki KAA taikymo pradžios, pagal KAA galėtų būti pateikiami rinkai neperprojektuoti, jeigu gamintojas, remdamasis kibernetinio saugumo rizikos vertinimu ir techniniais dokumentais, gali įrodyti, kad, atsižvelgiant į produkto su skaitmeniniais elementais numatytąją paskirtį ir pagrįstai numatomą naudojimą, pasiekiamas tinkamas jo kibernetinio saugumo lygis ir jis atitinka esminius kibernetinio saugumo reikalavimus.

37. Be to, naudinga paaiškinti atitikties vertinimo pareigų taikymą produktų su skaitmeniniais elementais, kurie rinkai pateikiami pradėjus taikyti KAA, tačiau yra pagaminti pagal iki jo taikymo pradžios datos suprojektuotą ir sukurtą tipą ar modelį, gamintojams. Pagal 13 straipsnio 12 dalį gamintojas, taikydamas atitinkamą atitikties vertinimo procedūrą, privalo įrodyti, kad jo produktas su skaitmeniniais elementais atitinka taikytinus esminius reikalavimus, ir į produkto techninius dokumentus įtraukti tai patvirtinančius įrodymus (VII priedo 6 punktas).

38. Tačiau šių reikalavimų taikymas turi būti aiškinamas atsižvelgiant į kibernetinio saugumo rizikos vertinimą ir produkto su skaitmeniniais elementais kibernetinio saugumo rizikos profilį. Visų pirma produktų su skaitmeniniais elementais, kurie buvo suprojektuoti iki KAA taikymo pradžios datos (tačiau rinkai pateikiami po šios datos) ir kuriems taikomos 32 straipsnio 1 dalyje nustatytos atitikties vertinimo procedūros, atveju, kai rizikos vertinimas rodo, kad produkte su skaitmeniniais elementais jau įdiegtos tinkamos ir veiksmingos saugumo priemonės, kuriomis mažinama su tuo produktu susijusi rizika, pareiga pateikti įrodymus atliekant atitikties vertinimo procedūrą neturėtų būti suprantama kaip reikalavimas, kad gamintojas pateiktų bandymų rezultatus, apimančius pirminius tokių produktų su skaitmeniniais elementais projektavimo ir kūrimo etapus. Tai nebūtų reikalinga, nes neprisidėtų prie paties produkto su skaitmeniniais elementais saugumo didinimo. Kai bandymai vis dėlto gali būti būtini, iš gamintojų nesitikima, kad jie pateiks visų produkto variantų bandymų įrodymus; tokius bandymus galima grupuoti pagal produktų su skaitmeniniais elementais grupes, kaip išsamiau aptariama *7.4* skirsnyje „*Rizikos vertinimų ir atitikties dokumentų pakartotinis naudojimas produktų su skaitmeniniais elementais grupėms*“.

39. Vis dėlto gamintojas turėtų pateikti įrodymus, kaip jis laikosi I priedo II dalyje nustatytų pažeidžiamumo valdymo procesų, pagal 13 straipsnio 3 dalį nuolat atnaujinti rizikos vertinimą, taip pat atlikti visas kitas KAA nustatytas pareigas, įskaitant pareigą pagal 13 straipsnio 18 dalį pateikti naudotojams informaciją ir instrukcijas.

12 pavyzdys. Gamintojas pateikia rinkai mikrovaldiklį, kuris buvo suprojektuotas ir sukurtas iki KAA taikymo pradžios datos. Mikrovaldiklis skirtas integruoti į įvairius elektroninius produktus su skaitmeniniais elementais, įskaitant produktus su skaitmeniniais elementais, turinčiais ryšio funkcijas.

Pradėjus taikyti KAA, gamintojas, prieš pateikdamas rinkai naujus mikrovaldiklio vienetus, pagal 13 straipsnio 2 dalį atlieka kibernetinio saugumo rizikos vertinimą. Atsižvelgdamas į mikrovaldiklio numatytąją paskirtį ir pagrįstai numatomą jo naudojimą, gamintojas nustato aktualią kibernetinio saugumo riziką, pavyzdžiui, neteisėtą prieigą, manipuliavimą programine įranga ar duomenimis ir netinkamą turimų sąsajų naudojimą.

Rizikos vertinimo rezultatai rodo, kad pirminės konstrukcijos mikrovaldiklyje jau yra įdiegtos tinkamos ir veiksmingos saugumo priemonės, skirtos nustatytai rizikai valdyti. Todėl gamintojas daro išvadą, kad produktas su skaitmeniniais elementais atitinka aktualius I priedo I dalyje nustatytus esminius reikalavimus ir kad nereikia jo perprojektuoti ar įdiegti papildomų saugumo funkcijų.

Kai neįmanoma parodyti, kaip į kibernetinio saugumo rizikos vertinimą buvo atsižvelgta pirminiame projektavimo ir kūrimo etape, gamintojas dokumentuoja esamą kibernetinio saugumo rizikos vertinimą ir paaiškina, kaip nustatyta rizika mažinama esama konstrukcija ir priemonėmis. Gamintojas neprivalo atkurti ankstesnių projektavimo ar bandymų dokumentų, nes tai nepadėtų didinti produkto su skaitmeniniais elementais kibernetinio saugumo. Kai kelių mikrovaldiklio variantų pagrindinė konstrukcija ir kibernetinio saugumo rizikos profilis yra tokie patys, gamintojas taip pat gali remtis reprezentatyviais įrodymais, apimančiais atitinkamą produktų grupę.

Gamintojas taip pat užtikrina, kad būtų laikomasi I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų, be kita ko, taikydamas procesus, skirtus pažeidžiamumui šalinti ir ištaisyti, ir pagal 13 straipsnio 3 dalį reguliariai peržiūrėdamas kibernetinio saugumo rizikos vertinimą.

Tokiomis aplinkybėmis mikrovaldiklis, suprojektuotas iki KAA taikymo pradžios datos, gali būti pateikiamas rinkai neperprojektuotas, jeigu gamintojas, remdamasis kibernetinio saugumo rizikos vertinimu ir techniniais dokumentais, gali įrodyti, kad, atsižvelgiant į mikrovaldiklio numatytąją paskirtį ir pagrįstai numatomą naudojimą, pasiekiamas tinkamas jo kibernetinio saugumo lygis ir jis atitinka taikomus esminius reikalavimus.

3. **LAISVOJI IR ATVIROJI PROGRAMINĖ ĮRANGA**

40. Kaip primenama *2.1* skirsnyje „*Pateikimas rinkai*“, KAA taikomas produktams su skaitmeniniais elementais, kurie pirmą kartą tiekiami ES rinkai vykdant komercinę veiklą (t. y. „pateikiami rinkai“), taip pat kiekvienu paskesniu atveju, kai tas pats produktas su skaitmeniniais elementais tiekiamas rinkai. Mėlynajame vadove (2.2 skirsnyje) paaiškinama, kad „komercinė veikla“ turi būti suprantama kaip prekių teikimas už atlygį arba nemokamai su verslu susijusiomis aplinkybėmis, o tai gali būti įvertinta tik kiekvienu konkrečiu atveju, atsižvelgiant į tiekimo reguliarumą, produkto savybes, tiekėjo ketinimus ir kt.

41. Tiekimui vykdant komercinę veiklą būdingos įvairios aplinkybės, išsamiai aptartos Mėlynajame vadove ir primenamos KAA 15 konstatuojamojoje dalyje. Jos gali apimti tiek tiesioginį mokesčio nustatymą, tiek „užmokesčio už techninės pagalbos paslaugas taikym[ą], kai tuo siekiama ne vien atgauti faktines išlaidas, siekiant monetizuoti, pavyzdžiui, teikiant programinės įrangos platformą, per kurią gamintojas gauna pajamų iš kitų paslaugų, kaip naudojimo sąlygą išreiškiant reikalavimą, kad asmens duomenys būtų tvarkomi kitais nei vien programinės įrangos saugumo, suderinamumo ar sąveikos gerinimo tikslais, arba priimant aukas, viršijančias su produkto su skaitmeniniais elementais projektavimu, kūrimu ir teikimu susijusias išlaidas“ (15 konstatuojamoji dalis) ([11]).

42. Tačiau KAA pripažįstama skirtingų „laisvosios ir atvirosios programinės įrangos“ (angl. *free and open-source software*, toliau – FOSS) kūrimo ir skelbimo būdų specifika ir pateikiamos tam tikros gairės, padedančios nustatyti, ar FOSS yra produktas su skaitmeniniais elementais, pateiktas rinkai (t. y. vykdant komercinę veiklą), kaip tai suprantama pagal KAA. Kaip paaiškinta 18 konstatuojamojoje dalyje, „nustatant tos veiklos komercinį ar nekomercinį pobūdį, neturėtų būti atsižvelgiama vien į aplinkybes, kuriomis produktas su skaitmeniniais elementais buvo sukurtas[,] ar kaip buvo finansuojamas jo kūrimas“. Konkrečiau, „siekiant užtikrinti, kad būtų aiškiai atskirti kūrimo ir tiekimo etapai, produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir už kuriuos jų gamintojai negauna pelno, teikimas neturėtų būti laikomas komercine veikla“.

([11]) Taip pat reikėtų priminti, kad nors produktai su skaitmeniniais elementais dažnai monetizuojami (taip pat) tvarkant asmens duomenis, asmens duomenų apsauga yra pagrindinė teisė, todėl asmens duomenys negali būti laikomi preke, kaip nurodyta 2019 m. gegužės 20 d. Europos Parlamento ir Tarybos direktyvos 2019/770 dėl tam tikrų skaitmeninio turinio ir skaitmeninių paslaugų teikimo sutarčių aspektų (OL L 136, 2019 5 22, p. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj) 24 konstatuojamojoje dalyje.

43. Todėl naudinga: i) paaiškinti, kas yra FOSS, ii) paaiškinti, kada laikoma, kad už ją atsako fizinis ar juridinis asmuo, ir iii) pateikti pavyzdžių, kurie padėtų suinteresuotiesiems subjektams suprasti, kada FOSS platinimas laikomas pateikimu rinkai. Kai FOSS nepateikiama rinkai, ji nepatenka į KAA taikymo sritį, išskyrus atvejus, kai ją skelbiantis subjektas yra juridinis asmuo, atitinkantis 3 straipsnio 14 punkte pateiktą atvirosios programinės įrangos valdytojo (toliau – valdytojas) apibrėžtį. Tokiu atveju jam taikomos tik 24 straipsnyje nustatytos pareigos.

44. 3 straipsnio 48 punkte FOSS apibrėžiama kaip „programinė įranga, kurios pirminiu kodu atvirai dalijamasi ir kuri pateikiama pagal laisvąją atvirojo kodo licenciją, kurioje numatytos visos teisės padaryti, kad ji būtų laisvai prieinama, naudojama, keičiama ir pakartotinai platinama“. Nors šiose gairėse nenurodomos konkrečios laisvosios atvirojo kodo licencijos, kurios atitiktų 3 straipsnio 48 punkte nustatytą apibrėžtį, iš tos nuostatos formuluotės matyti, kad KAA taikymo tikslais FOSS laikoma tik tokia programinė įranga, kuri vienu metu atitinka abi šias sąlygas: i) programinė įranga yra prieinama pagal laisvąją atvirojo kodo licenciją, kuria suteikiamos visos 3 straipsnio 48 punkte nurodytos teisės, ir ii) jos pirminiu kodu atvirai dalijamasi.

45. Reikalavimas, kad programinė įranga pagal licenciją būtų „laisvai prieinama, naudojama, keičiama ir pakartotinai platinama“, atspindi tradicinę FOSS sampratą, pagal kurią naudotojai turi turėti prieigą prie pirminio kodo, naudoti programinę įrangą be nepagrįstų apribojimų, ją keisti ir platinti pirmines arba pakeistas versijas. Todėl prieiga prie pirminio kodo yra būtina sąlyga naudotis kitomis teisėmis: neturint prieigos prie pirminio kodo, praktiškai neįmanoma programinės įrangos pakeisti ar prasmingai pakartotinai panaudoti.

46. Tačiau 3 straipsnio 48 punkte nurodomos ne vien licencijos sąlygos, nes jame aiškiai reikalaujama, kad pirminiu kodu būtų „atvirai dalijamasi“. Žodžių junginys „atvirai dalijamasi“ reiškia, kad pirminis kodas turi būti viešai prieinamas – nesvarbu, ar pirmesnėse, ar tolesnėse tiekimo grandinės grandyse, – o ne teikiamas tik ribotai ar su tam tikromis sąlygomis. Todėl programinė įranga, kuri platinama pagal laisvąją atvirojo kodo licenciją, tačiau kurios pirminiu kodu dalijamasi (arba leidžiama dalytis) tik su klientais, kurie už tai moka, ar ribota naudotojų grupe, neturi būti laikoma FOSS, kaip ji suprantama 3 straipsnio 48 punkte. Taigi KAA taikymo tikslais FOSS turėtų būti laikoma tik tokia programinė įranga, kurios pirminis kodas yra viešai prieinamas ir licencijuotas pagal laisvąją atvirojo kodo licenciją, kuria suteikiamos visos 3 straipsnio 48 punkte nurodytos teisės.

3.1. **Nustatymas, ar už laisvąją ir atvirąją programinę įrangą atsako konkretus asmuo**

47. KAA nustatomos pagrindinės pareigos ekonominės veiklos vykdytojams, ES rinkai tiekiantiems produktus su skaitmeniniais elementais. Jame gamintojas apibrėžiamas kaip fizinis arba juridinis asmuo, kuris produktą su skaitmeniniais elementais tiekia savo vardu arba naudodamas savo prekių ženklą ir tai daro vykdydamas komercinę veiklą (taigi pateikia jį rinkai). Importuotojas atitinkamai yra fizinis arba juridinis asmuo, kuris tiekia ne ES įsisteigusio asmens produktą su skaitmeniniais elementais ir tai daro vykdydamas komercinę veiklą (taigi pateikia jį rinkai). Valdytojams nustatytos pareigos taikomos juridiniam asmeniui, kuris tiekia komercinei veiklai skirtą FOSS ([12]), tačiau nepateikia jos rinkai, kaip tai suprantama pagal KAA.

48. Todėl siekiant nustatyti, ar fizinis arba juridinis asmuo pateikia FOSS ES rinkai, pirmiausia reikia išsiaiškinti, ar tas fizinis arba juridinis asmuo iš tiesų tiekia FOSS. Siekiant teisingai nustatyti pagal KAA taikytinas pareigas, būtina nustatyti, ar fizinis arba juridinis asmuo iš tiesų atlieka FOSS tiekimo veiksmą. Iš tiesų, kaip priminta 18 konstatuojamojoje dalyje, KAA netaikomas fiziniams arba juridiniams asmenims, kurie prie produktų su skaitmeniniais elementais, laikomų FOSS ir nepriklausančių jų atsakomybei, prisideda teikdami pirminį kodą.

([12]) Tai yra būtina, tačiau nepakankama sąlyga, kad juridinis asmuo būtų laikomas atvirosios programinės įrangos valdytoju, nes 3 straipsnio 14 punkte pateiktoje apibrėžtyje nustatytos ir papildomos sąlygos, kurias juridinis asmuo turi atitikti, kad būtų laikomas valdytoju.

49. Atsižvelgiant į FOSS kūrimo specifiką (dažnai dalyvauja daug prisidedančiųjų asmenų, taikomi decentralizuoto bendradarbiavimo modeliai ir prisidėjimas skiriamas nuo sprendimų priėmimo), naudinga paaiškinti, kad atsakomybė už FOSS tenka tiems fiziniams arba juridiniams asmenims, kurie ją skelbia ir iš esmės kontroliuoja jos kūrimą, versijų išleidimą ir sprendimus dėl platinimo. Tokie asmenys dažnai vadinami techninės priežiūros vykdytojais (angl. *maintainers*). Asmenys, kurie prisideda teikdami pirminį kodą, tačiau nekontroliuoja versijų išleidimo, plėtros planų ar valdymo sprendimų, laikomi prisidedančiaisiais asmenimis (angl. *contributors*); tokiais atvejais atsakomybė už FOSS tenka ne jiems, nors jie prie jos prisidėjo teikdami kodą. Vien techninių leidimų, pavyzdžiui, teisės tiesiogiai įkelti pakeitimus į saugyklą (angl. *commit access*), nepakanka siekiant nustatyti, ar atsakomybė už FOSS tenka tam asmeniui; atsakomybė tenka tiems, kurie FOSS skelbia ir kontroliuoja.

13 pavyzdys. Individualus kūrėjas arba įmonės darbuotojas FOSS projektui pateikia pakeitimų įtraukimo prašymą arba pakeitimų sujungimo prašymą, kuriame pateikiama saugumo pataisa arba nauja funkcija. Projekto techninės priežiūros vykdytojai peržiūri kodą, ji priima ir sujungia su pagrindinės saugyklos duomenimis, o vėliau įtraukia jį į naują programinės įrangos versiją. Pagal šį scenarijų pakeitimų įtraukimo prašymą pateikęs asmuo laikomas prisidedančiuoju asmeniu ir jam KAA netaikomas. Nors tas asmuo prisidėjo teikdamas pirminį kodą, jis iš esmės nekontroliuoja programinės įrangos kūrimo, versijų išleidimo ar sprendimų dėl platinimo.

3.2. **Nustatymas, ar laisvoji ir atviroji programinė įranga pateikiama ES rinkai**

50. Nustačius, kad atsakomybė už FOSS tenka fiziniam arba juridiniam asmeniui, reikia nustatyti, ar tas asmuo ją tiekia vykdydamas komercinę veiklą ir ar dėl to toks tiekimas laikomas pateikimu rinkai.

3.2.1. *Mokesčio nustatymas*

51. Kai FOSS tiekiantis fizinis arba juridinis asmuo ima mokestį už pačią programinę įrangą (pvz., ima mokestį už iš anksto sukompiliuotus dvejetainius failus), tas asmuo produktą su skaitmeniniais elementais pateikia rinkai. Todėl FOSS rinkai pateikiantis asmuo pagal KAA yra gamintojas.

52. FOSS gamintojai dažnai nemokamai tiekia ir tokios programinės įrangos versijas, dažnai vadinamas bendruomeninėmis (angl. *community*) versijomis, kurių programinio kodo bazė yra (beveik) identiška mokamai versijai. Tačiau šie produktai su skaitmeniniais elementais yra skirtingi produktai: mokama versija vienaip ar kitaip monetizuojama (pvz., nustatant mokestį arba kitomis šiame skirsnyje aptartomis priemonėmis), todėl laikoma pateikta rinkai ir jos atžvilgiu taikomos gamintojo pareigos. Nemokamai teikiama versija (arba bendruomeninė versija) nėra monetizuojama, todėl KAA taikymo tikslais nelaikoma pateikta rinkai. Tas pats taikoma ir tais atvejais, kai mokama versija yra išplėsta (angl. *enhanced*) komercinė versija, kuria išplečiama nemokamai teikiamos versijos programinio kodo bazė, arba kuria ši nemokama versija įtraukiama į platesnės aprėpties produktą su skaitmeniniais elementais, pavyzdžiui, taikant vadinamąjį atvirojo branduolio (angl. *open core*) modelį.

53. Jeigu bendruomeninę versiją teikiantis asmuo yra juridinis asmuo, tam juridiniam asmeniui taip pat taikomos valdytojams nustatytos pareigos, kiek tai susiję su jo nemokamai teikiama versija (bendruomenine versija). Jeigu subjektas yra fizinis asmuo, nemokamai teikiama versija (bendruomeninė versija) nepatenka į KAA taikymo sritį.

3.2.2. *Kitų paslaugų monetizavimas arba poreikis tvarkyti asmens duomenis*

54. FOSS skelbiantis fizinis arba juridinis asmuo taip pat gali ją pateikti rinkai (t. y. tiekti ją vykdydamas komercinę veiklą), kai jis tą programinę įrangą teikia kaip priemonę, per kurią monetizuoja kitus produktus su skaitmeniniais elementais ar paslaugas, arba kai jis nustato naudojimosi sąlygą, kad asmens duomenys būtų tvarkomi kitais negu vien programinės įrangos saugumo, suderinamumo ar sąveikumo gerinimo tikslais.

14 pavyzdys. Fizinis arba juridinis asmuo paskelbia laisvąją ir atvirąją elektroninės prekyvietės taikomąją programą. Ta taikomoji programa yra nemokama ir suteikia naudotojams galimybę per ją įsigyti prekių arba paslaugų. Taikomoji programa suteikia galimybę ją paskelbusiam asmeniui monetizuoti kitus per ją siūlomus produktus su skaitmeniniais elementais ir paslaugas (pvz., gaunant pajamų iš reklamos, komisinių ar abonentinių mokesčių). Todėl laikoma, kad taikomoji programa pateikiama rinkai vykdant komercinę veiklą.

15 pavyzdys. Fizinis arba juridinis asmuo paskelbia laisvąją ir atvirąją VPN programinę įrangą. Taikomoji programa yra prieinama nemokamai, tačiau suteikia naudotojams galimybę už užmokestį naudotis papildomais serveriais arba specialiai jiems skirtais IP adresais. Tokia taikomoji programa leidžia tam asmeniui monetizuoti kitas per ją siūlomas paslaugas, todėl laikoma, kad ji pateikiama rinkai vykdant komercinę veiklą.

16 pavyzdys. Fizinis arba juridinis asmuo paskelbia laisvąją ir atvirąją fizinio aktyvumo stebėjimo taikomąją programą. Taikomoji programa yra prieinama nemokamai, tačiau naudotis ja galima tik su sąlyga, kad naudotojo asmens duomenys bus tvarkomi tokiais tikslais kaip tikslinė reklama arba analitika, nesusijusi su programinės įrangos saugumu, suderinamumu ar sąveikumu. Kadangi toks duomenų tvarkymas nustatomas kaip naudojimosi sąlyga, laikoma, kad taikomoji programa pateikiama rinkai vykdant komercinę veiklą.

3.2.3. *Palaikymo paslaugos*

55. Vien tai, kad FOSS skelbiantis fizinis arba juridinis asmuo taip pat siūlo mokamas jos palaikymo paslaugas, savaime nereiškia, kad produktas su skaitmeniniais elementais tiekiamas vykdant komercinę veiklą. Palaikymo paslaugos gali apimti, pavyzdžiui, konsultavimo, mokymo ar profesines paslaugas, susijusias su kliento naudojimusi programine įranga, jos dokumentacija, konfigūravimu ir diegimu.

56. Lemiamas veiksnys yra tai, ar prieiga prie pačios FOSS (t. y. produkto su skaitmeniniais elementais teikimas), įskaitant jos techninę priežiūrą, priklauso nuo atlygio mokėjimo, o ne vien tai, kad siūlomos su laisvai prieinamu produktu su skaitmeniniais elementais susijusios profesinės paslaugos, kaip nurodyta KAA 18 konstatuojamojoje dalyje („produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir už kuriuos jų gamintojai negauna pelno, teikimas neturėtų būti laikomas komercine veikla“). Jeigu FOSS galima laisvai parsisiųsti ir įsidiegti, o naudotojai gali savo nuožiūra atskirai įsigyti profesinių paslaugų, nelaikoma, kad tokia FOSS pateikiama rinkai.

57. Tačiau kai kuriais atvejais prieiga prie konkrečios produkto su skaitmeniniais elementais versijos, apimančios tam tikrus papildomus pranašumus, pavyzdžiui, techninę pagalbą ar veikimo optimizavimą, suteikiama tik už atlygį. Tokiais atvejais toks teikimas yra monetizuojamas produkto su skaitmeniniais elementais tiekimas vykdant komercinę veiklą, todėl laikoma, kad produktas pateikiamas rinkai. Tai apima atvejus, kai mokama laida arba įmonėms skirta versija teikiama pagal komercinį susitarimą, nepriklausomai nuo to, ar funkciškai lygiavertė programinė įranga taip pat yra prieinama nemokamai pagal laisvąją atvirojo kodo licenciją.

17 pavyzdys. Fizinis arba juridinis asmuo paskelbia laisvąją ir atvirąją operacinę sistemą ir kartu pasiūlo mokamą tos operacinės sistemos versiją, į kurią įtrauktos palaikymo paslaugos, tokios kaip techninė pagalba ar veikimo optimizavimas. Laikoma, kad mokama operacinės sistemos versija pateikiama rinkai vykdant komercinę veiklą.

18 pavyzdys. Fizinis arba juridinis asmuo paskelbia laisvąją ir atvirąją komandų eilutės priemonę. Priemonė yra laisvai prieinama, ją gali parsisiųsti ir įsidiegti bet kas. Tas fizinis arba juridinis asmuo atskirai siūlo profesines paslaugas, tokias kaip neprivalomos konsultavimo paslaugos, skirtos naudotojams mokyti ir padėti jiems įdiegti bei naudoti šią priemonę. Tokia FOSS nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA.

58. Visų pirma tais atvejais, kai FOSS skelbia fiziniai asmenys, techninės pagalbos, tiesiogiai susietos su prieiga prie produkto su skaitmeniniais elementais, teikimas vis vien nebūtų laikomas komercine veikla, jeigu, kaip nurodyta KAA 15 konstatuojamojoje dalyje, nustatyta kaina skirta tik faktinėms išlaidoms padengti. Tokios faktinės išlaidos apima įvairias su tos programinės įrangos projektavimu, kūrimu ir priežiūra susijusias išlaidas, įskaitant pagrįstas to asmens pragyvenimo išlaidas. Todėl vien šios aplinkybės nepakanka, kad fizinis asmuo, skelbiantis FOSS ir teikiantis techninę pagalbą tam, kad padengtų savo išlaidas ir gautų teisingą atlygį, būtų laikomas pateikiančiu tą programinę įrangą ES rinkai.

59. Fizinis arba juridinis asmuo, teikiantis techninę pagalbą, susijusią su FOSS, nepriklausančia jo atsakomybei, nelaikomas pateikiančiu tą programinę įrangą rinkai, išskyrus atvejus, kai teikdamas tokią pagalbą tas asmuo iš esmės pakeičia FOSS, kaip nustatyta 22 straipsnyje.

19 pavyzdys. Paslaugų teikėjas neskelbia FOSS, tačiau padeda klientui ją įdiegti kliento patalpose esančiame serveryje. Tai darant ta FOSS iš esmės nepakeičiama, todėl nelaikoma, kad paslaugų teikėjas FOSS pateikia rinkai.

3.2.4. *Aukos*

60. FOSS projektus skelbiantys fiziniai arba juridiniai asmenys įprastai suteikia galimybę tos programinės įrangos naudotojams savanoriškai paaukoti pinigų ir taip išreikšti padėką projektą skelbiančiam asmeniui ar asmenims ir kartu padėti užtikrinti, kad projektas būtų ir toliau aktyviai palaikomas.

61. Kaip nurodyta KAA 15 konstatuojamojoje dalyje, „[a]ukų priėmimas be ketinimo gauti pelno neturėtų būti laikomas komercine veikla“. Vien tai, kad pateikiama nuoroda į aukų rinkimo platformą ar naudojamos panašios priemonės aukoms rinkti, neturėtų būti vertinama kaip siekis gauti pelno, net jei paaukotų pinigų suma viršija vien su produkto su skaitmeniniais elementais projektavimu, kūrimu ir teikimu susijusias išlaidas. Tokios išlaidos apima pagrįstą atlygį juridinio asmens samdomiems prie projekto prisidedantiems asmenims ir (arba) pagrįstas fizinio asmens pragyvenimo išlaidas. Aukų dydis dėl pačios jų esmės laikui bėgant kinta, todėl vertinant, ar vien iš paaukotų pinigų monetizuojama FOSS laikoma pateikta rinkai, reikėtų tam tikro lankstumo. Todėl mažai tikėtina, kad vien iš aukų palaikoma FOSS būtų laikoma pateikta rinkai, kaip tai suprantama pagal KAA.

20 pavyzdys. Fizinis arba juridinis asmuo paskelbia FOSS priemonę viešoje internetinėje saugykloje ir pagal laisvąją atvirojo kodo licenciją leidžia bet kam ją parsisiųsti, naudoti, keisti ir platinti. Ją paskelbęs asmuo kviečia naudotojus savanoriškai aukoti per aukų rinkimo platformą, kad paremtų tolesnį projekto plėtojimą ir priežiūrą. Prieiga prie programinės įrangos, jos pirminio kodo ir naujinių nepriklauso nuo to, ar aukojama, ar ne. Tokia FOSS nelaikoma tiekiama vykdant komercinę veiklą ir nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA.

62. Vis dėlto tam tikrais atvejais iš aukų palaikoma FOSS gali būti laikoma pateikta rinkai. Taip yra tuomet, kai, visapusiškai įvertinus aplinkybes, aukos *de facto* prilygsta mokesčio už prieigą prie produkto su skaitmeniniais elementais arba naudojimąsi tam tikromis jo funkcijomis nustatymui. Visų pirma taip gali būti tais atvejais, kai prieiga prie FOSS, esminių jos funkcijų ar naujinių praktiškai priklauso nuo aukojimo arba kai su aukomis siejama sutartinė nauda ar išskirtiniai pranašumai, neapsiribojantys įprastomis bendruomenės nariams teikiamomis privilegijomis.

21 pavyzdys. Fizinis arba juridinis asmuo paskelbia programinės įrangos produktą su skaitmeniniais elementais pagal laisvąją atvirojo kodo licenciją, tačiau parsisiunčiamas versijas ir saugumo naujinius teikia tik pinigų paaukojusiems naudotojams. Aukos neskyrę naudotojai neturi prieigos prie naujausios programinės įrangos versijos.

Tokiu atveju aukojimas faktiškai yra prieigos prie produkto su skaitmeniniais elementais sąlyga, todėl prilygsta mokesčio nustatymui. Taigi tokia FOSS laikoma pateikta rinkai, kaip tai suprantama pagal KAA.

22 pavyzdys. Fizinis arba juridinis asmuo viešai paskelbia FOSS pirminį kodą, tačiau iš anksto sukompiliuotus dvejetainius failus, reguliarius atnaujinimus ir garantuojamas saugumo pataisas teikia tik aukotojams. Tokiu atveju aukos yra susietos su prieiga prie esminių produkto su skaitmeniniais elementais aspektų ir yra atlygis už to produkto tiekimą. Todėl tokia FOSS laikoma pateikta rinkai vykdant komercinę veiklą.

3.2.5. *Laisvosios ir atvirosios programinės įrangos finansavimas*

63. Vien pagal tai, kad trečioji šalis sumokėjo už FOSS kūrimą, jį rėmė ar kitaip finansavo, negalima spręsti, ar ta FOSS yra pateikta rinkai. FOSS ekosistemoje įprasta, kad pavieniai kūrėjai, fondai ar bendruomenės gauna finansavimą iš įmonių, viešųjų įstaigų ar kitų rėmėjų tam, kad kurtų konkrečias funkcijas, taisytų riktus ar prižiūrėtų ypatingos svarbos komponentus. Toks finansavimas gali būti įvairių formų, įskaitant dotacijas, atlygius už riktų aptikimą, rėmimą, paslaugų sutartis ar apmokamus plėtros darbus.

64. Kaip jau minėta, KAA 18 konstatuojamojoje dalyje paaiškinama, kad nustatant tokios veiklos komercinį pobūdį neturėtų būti atsižvelgiama vien į aplinkybes, kuriomis produktas su skaitmeniniais elementais buvo sukurtas, ar į tai, kaip jo kūrimas buvo finansuojamas.

65. Todėl, kai FOSS yra viešai bendrinama ir laisvai prieinama visiems, kad ją būtų galima pasiekti, naudoti, keisti ir platinti, aplinkybė, kad komercinis subjektas galėjo finansuoti tą projektą, neturėtų turėti reikšmės nustatant, ar programinė įranga yra pateikta rinkai. Iš tiesų, jei tokia FOSS nėra monetizuojama jokiu kitu būdu, ji neturi būti laikoma pateikta rinkai. Kai FOSS kūrimą finansavusi įmonė (kaip ir bet kuri kita įmonė) integruoja ją į savo produktą su skaitmeniniais elementais, ta įmonė pagal KAA 13 straipsnio 5 dalį turi atlikti išsamų patikrinimą.

23 pavyzdys. Individualus kūrėjas paskelbia FOSS projektą ir aktyviai jį prižiūri. Gamintojas A paprašo individualaus kūrėjo į tą FOSS įtraukti konkrečią funkciją ir finansuoja jos kūrimą. Kūrėjas šią funkciją įtraukia į FOSS programinio kodo bazę, ja atvirai dalijasi ir suteikia galimybę visiems laisvai ją pasiekti, naudoti, keisti ir platinti. Tas individualus kūrėjas nelaikomas pateikusiu tą FOSS rinkai. Jei gamintojas integruoja FOSS į savo produktą su skaitmeniniais elementais, jis pagal 13 straipsnio 5 dalį turi atlikti išsamų patikrinimą.

3.2.6. *Ne pelno tikslais įsteigti pelno nesiekiantys subjektai*

66. Kai FOSS skelbiantis juridinis asmuo yra pelno nesiekianti organizacija, „įsteigta taip, kad būtų užtikrinta, jog visos pajamos atskaičius išlaidas būtų naudojamos ne pelno tikslams siekti“ (KAA 18 konstatuojamoji dalis), jos skelbiama FOSS nelaikoma pateikta rinkai. Jei toks juridinis asmuo atitinka „valdytojo“ apibrėžtį, jam taikomos atitinkamos pareigos (KAA 24 straipsnis).

24 pavyzdys. Juridinis asmuo paskelbia laisvąją ir atvirąją saityno naršyklę, kuri tiesiogiai monetizuojama pagal partnerystės su paieškos sistemų teikėjais susitarimus, tačiau visos jos generuojamos pajamos, atskaičius išlaidas, naudojamos ne pelno tikslais. Naršyklė nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA. Ją skelbiančiam juridiniam asmeniui taikomos valdytojams nustatytos pareigos.

3.2.7. *Integravimas, kurį atlieka kiti gamintojai*

67. Kai kuriais atvejais FOSS paskelbia aiškiai identifikuojamas fizinis arba juridinis asmuo, tačiau ta FOSS yra „skirt[a] kitiems gamintojams integruoti į savo produktus su skaitmeniniais elementais“. Tokiais atvejais FOSS nelaikoma pateikta ES rinkai, išskyrus atvejus, kai ją skelbiantis asmuo (t. y. pirminis gamintojas) ją taip pat monetizuoja, kaip aprašyta pirmesniuose šių gairių skirsniuose.

68. Kai tokia FOSS nėra pateikiama rinkai, ją skelbiančiam juridiniam asmeniui būtų taikomos valdytojams nustatytos pareigos, jeigu jis nuolat ją palaiko, kaip nustatyta sąvokos „valdytojas“ apibrėžtyje.

25 pavyzdys. Juridinis asmuo paskelbia FOSS biblioteką, skirtą naudotojo sąsajoms kurti. Jis nemonetizuoja šios bibliotekos teikimo, tačiau integruoja ją į vieną iš savo produktų su skaitmeniniais elementais, o šis yra pateikiamas rinkai. Biblioteka nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA, tačiau ji yra skirta integruoti į produktus su skaitmeniniais elementais. Ją skelbiantis juridinis asmuo yra jos valdytojas.

26 pavyzdys. Juridinis asmuo pateikia rinkai operacinę sistemą ir taip pat skelbia FOSS bibliotekas, kurios yra tos operacinės sistemos naudotojams skirti pavyzdinės realizacijos modeliai. Juridinis asmuo nemonetizuoja FOSS bibliotekų, kurios skirtos integruoti į kitus produktus su skaitmeniniais elementais. Jas skelbiantis juridinis asmuo yra tų FOSS bibliotekų valdytojas.

3.3. **Atvirosios programinės įrangos valdytojai**

69. KAA nustatoma nauja teisinė „atvirosios programinės įrangos valdytojo“ kategorija, atsižvelgiant į „daugelio produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir kurie skelbiami, bet nepateikiami rinkai, kaip tai suprantama [KAA], svarbą kibernetiniam saugumui“ (KAA 19 konstatuojamoji dalis).

70. Kai kuriais atvejais FOSS paskelbia, tačiau tiekimo rinkai, kaip tai suprantama pagal KAA, nevykdo juridinis asmuo, „kurio tikslas ar užduotis – sistemingai nuolat teikti paramą [FOSS] [...], [...] skirt[ai] komercinei veiklai, kūrimui ir kuris užtikrina tų produktų gyvybingumą“ (KAA 3 straipsnio 14 punktas). Tokiais atvejais tam juridiniam asmeniui taikomos valdytojams nustatytos pareigos.

71. Valdytojas apibrėžiamas kaip „juridinis asmuo, kuris nėra gamintojas“, nes gamintojas pagal apibrėžtį yra fizinis arba juridinis asmuo, kuris savo vardu arba naudodamas savo prekių ženklą pateikia rinkai produktus su skaitmeniniais elementais („parduoda juos“). Juridinis asmuo gali būti tik tų produktų su skaitmeniniais elementais, kurie laikomi FOSS ir yra skelbiami, tačiau nėra tiekiami rinkai, kaip tai suprantama pagal KAA, valdytojas. Todėl valdytojo samprata taikoma konkrečioms FOSS, kurios „galiausiai yra skirt[os] komercinei veiklai, pavyzdžiui, integravimui į komercines paslaugas arba į monetizuotus produktus su skaitmeniniais elementais“ (KAA 19 konstatuojamoji dalis ([13])), tačiau nėra tiekiamos rinkai, kaip tai suprantama pagal KAA, ir kurių sistemingą palaikymą užtikrina jas skelbiantis juridinis asmuo.

72. Tai, kad juridinis asmuo yra vienos konkrečios FOSS valdytojas, nebūtinai reiškia, kad jis taip pat yra kitų savo skelbiamų FOSS valdytojas. Taip pat tai, kad juridinis asmuo yra vienos konkrečios FOSS gamintojas, nereiškia, kad jis negali būti kitų FOSS valdytojas. Tai apima ir tos pačios FOSS bendruomeninių versijų teikimą, kaip aprašyta *3.2.1* skirsnyje „*Mokesčio nustatymas*“.

73. Todėl juridinis asmuo tuo pačiu metu gali būti vienos konkrečios FOSS valdytojas (kai valdytojas sistemingai nuolat teikia palaikymo paslaugas ir užtikrina programinės įrangos gyvybingumą) ir kitos konkrečios FOSS gamintojas (kai jis ją pateikia rinkai). Kitaip tariant, tam pačiam juridiniam asmeniui gali tekti atlikti skirtingus vaidmenis, susijusius su skirtingais FOSS projektais.

74. Dėl kiekvienos konkrečios savo skelbiamos FOSS juridinis asmuo turės nustatyti, ar ta FOSS laikoma pateikta rinkai, kaip tai suprantama pagal KAA. Jeigu taip, juridinis asmuo laikomas tos programinės įrangos gamintoju. Jeigu FOSS nelaikoma pateikta rinkai, juridinis asmuo gali būti jos valdytojas, jei ta programinė įranga yra skirta komercinei veiklai ir juridinis asmuo užtikrina nuolatinę jos priežiūrą pagal valdytojo apibrėžtį ([14]).

3.3.1. *Nuolatinė parama ir FOSS gyvybingumo užtikrinimas*

75. 19 konstatuojamojoje dalyje paaiškinama, kad nuolatinės paramos produkto su skaitmeniniais elementais kūrimui teikimas gali apimti, be kita ko: i) programinės įrangos kūrimo bendradarbiavimo platformų prieglobą ir valdymą; ii) pirminio kodo arba programinės įrangos prieglobą; iii) produktų su skaitmeniniais elementais, laikomų FOSS, administravimą ar valdymą, ir iv) vadovavimą tokių produktų su skaitmeniniais elementais kūrimui.

76. Taip gali būti, pavyzdžiui, kai juridinis asmuo kuria FOSS tam, kad ją integruotų į savo produktus su skaitmeniniais elementais, o vėliau ją paskelbia, tačiau nepateikia rinkai. Tai taip pat aptariama *3.2.7* skirsnyje „*Integravimas, kurį atlieka* kiti gamintojai“. Tokiu atveju juridinis asmuo nėra programinės įrangos gamintojas, tačiau gali būti jos valdytojas. Be to, kaip paaiškinta ir pirmesniuose skirsniuose, juridinis asmuo, kuris skelbia nemokamą (arba bendruomeninę) ir monetizuojamą tos pačios FOSS versiją, laikomas tos nemokamos (arba bendruomeninės) versijos valdytoju ir monetizuojamos versijos gamintoju.

77. Panašiai juridinis asmuo, kuris monetizuoja FOSS, tačiau yra pelno nesiekiantis subjektas, kurio visos pajamos, atskaičius išlaidas, naudojamos ne pelno tikslams (todėl, kaip aptarta *3.2.6* skirsnyje „*Ne pelno* tikslais įsteigti pelno nesiekiantys subjektai“, jo FOSS nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA), yra savo skelbiamos FOSS valdytojas.

78. Be to, kai kurie fondai siūlo įvairių valdymo formų bendradarbiavimo platformas, kurios suteikia gamintojams galimybę reguliariai prisidėti prie FOSS kūrimo ir (arba) kurias reguliariai finansuoja gamintojai. Tokie fondai turi būti laikomi konkrečių FOSS, kurios yra skirtos komercinei veiklai ir kurioms fondas nuolat teikia paramą, valdytojais. Tačiau, kaip paaiškinta *3.3* skirsnyje „*Atvirosios programinės įrangos* valdytojai“, tokiam fondui gali būti netaikomos jokios KAA nustatytos pareigos kitų konkrečių FOSS, kurioms jis teikia prieglobą, atžvilgiu tais atvejais, kai jis neteikia sistemingos paramos konkrečiai FOSS, neužtikrina jos gyvybingumo ir (arba) ta konkreti programinė įranga nėra skirta komercinei veiklai.

([13]) Ši sąvoka taip pat atsispindi formuluotėje „skirt[a] komercinei veiklai“, vartojamoje KAA 3 straipsnio 14 punkte pateiktoje „atvirosios programinės įrangos valdytojo“ apibrėžtyje.

([14]) Juridiniam asmeniui taip pat gali būti netaikomos jokios KAA nustatytos pareigos tais atvejais, kai: i) konkreti FOSS nėra pateikta rinkai, kaip tai suprantama pagal KAA, ir ii) juridinis asmuo tos konkrečios FOSS atžvilgiu neatitinka valdytojo apibrėžties.

79. „Nuolatinės paramos“, kurią fondai ir panašios organizacijos teikia konkretiems FOSS projektams, pobūdis gali labai skirtis. Pavyzdžiui, kai kurie juridiniai subjektai teikia tik netechninę paramą, pavyzdžiui, administruoja projektų prekių ženklus, nustato valdymo taisykles, organizuoja bendruomenės renginius ar renka aukas. Kiti subjektai taip pat teikia projektui vykdyti būtiną pagrindinę IT infrastruktūrą, pavyzdžiui, užtikrina pirminio kodo saugyklų prieglobą, teikia versijų kontrolės sistemas ar generuoja pasirašymo raktus. Dar kiti teikia platesnio masto paramą, t. y. aktyviai skiria projektui inžinerinius išteklius, pavyzdžiui, įdarbina kūrėjus, koordinuoja kūrimo darbus, peržiūri ar sujungia programinį kodą, valdo versijų išleidimą arba tvarko pranešimus apie pažeidžiamumą ir saugumo pataisas. Nors visi juridiniai subjektai, pagal KAA laikomi valdytojais, privalo atlikti 24 straipsnio 1 ir 2 dalyse nustatytas pareigas, 14 straipsnio 1, 3 ir 8 dalyse nustatytų pareigų taikymo tokiems juridiniams subjektams apimtis pagal 24 straipsnio 3 dalį priklauso nuo jų teikiamos paramos pobūdžio.

80. Pavyzdžiui, valdytojas, teikiantis tik netechninę paramą, pagal apibrėžtį nedalyvauja kuriant produktą su skaitmeniniais elementais, todėl neprivalo pranešti apie aktyviai išnaudojamą pažeidžiamumą. Toks valdytojas taip pat neteikia jokių tinklų ar informacinių sistemų, skirtų tokiems produktams su skaitmeniniais elementais kurti, todėl neprivalo apie didelius incidentus pranešti ENISA ir CSIRT arba paveiktiems naudotojams. Vis dėlto, jei valdytojas sužino apie aktyviai išnaudojamą pažeidžiamumą (pvz., gavęs pranešimą iš išorės šaltinių, tokių kaip saugumo tyrėjai), jis pagal savo kibernetinio saugumo politiką turėtų perduoti šią informaciją produkto su skaitmeniniais elementais techninės priežiūros vykdytojams. Produktų su skaitmeniniais elementais techninės priežiūros vykdytojai ir (arba) valdytojai taip pat turėtų apsvarstyti galimybę savanoriškai pranešti apie pažeidžiamumą pagal 15 straipsnį.

81. Kita vertus, kai valdytojas teikia tam tikrų produktų su skaitmeniniais elementais pagrindinę IT infrastruktūrą, jis pagal 14 straipsnio 3 dalį privalo ENISA ir CSIRT pranešti apie visus su ta infrastruktūra susijusius didelius incidentus, kurie daro poveikį produktų su skaitmeniniais elementais saugumui. Kai tikslinga, jis taip pat privalo informuoti visus naudotojus (pvz., paskelbdamas bendrą pranešimą). Kaip nurodyta pirmesniame punkte, nors valdytojas neprivalo pranešti apie jam žinomą aktyviai išnaudojamą pažeidžiamumą, jis turėtų skatinti tinkamą pažeidžiamumo valdymą ir apsvarstyti galimybę savanoriškai pranešti pagal 15 straipsnį.

82. Galiausiai, kai valdytojas taip pat teikia inžinerinius išteklius konkretiems produktams su skaitmeniniais elementais, jis privalo: i) pagal 14 straipsnio 1 dalį pranešti apie jam žinomą aktyviai išnaudojamą pažeidžiamumą ir, ii) kai tikslinga, informuoti visus naudotojus. Jei valdytojas palaiko tiesioginius santykius su paveiktais naudotojais, jis pagal 14 straipsnio 8 dalį taip pat privalo juos informuoti tiesiogiai.

83. Kai subjektas nustoja sistemingai ir nuolat teikti paramą konkrečiai FOSS, jis gali nebeatitikti valdytojo apibrėžties, todėl gali nebeturėti atitinkamų pareigų. Tokiais atvejais subjektas raginamas aiškiai pranešti apie savo statuso pasikeitimą tos konkrečios FOSS atžvilgiu.

84. Tam tikrais atvejais subjektas, kuris buvo konkretaus projekto valdytojas, gali nuspręsti tiesiogiai monetizuoti tą projektą, taip pateikdamas produktą su skaitmeniniais elementais rinkai ir dėl to privalėdamas vykdyti gamintojo pareigas pagal KAA. Tokiomis aplinkybėmis tas subjektas laikomas produkto su skaitmeniniais elementais gamintoju nuo tos dienos, kurią tą produktą pateikia rinkai, (tačiau tai netaikoma ankstesnėms versijoms, kurių atžvilgiu jis veikė kaip valdytojas).

3.4. **Prisidedantys asmenys ir tolesni naudojimo būdai**

85. Kaip jau minėta *3.1* skirsnyje „*Nustatymas, ar už laisvąją ir atvirąją* programinę įrangą atsako konkretus asmuo“, KAA paaiškinama, kad jis netaikomas „fiziniams ar juridiniams asmenims, kurie pirminiu kodu prisideda prie produktų su skaitmeniniais elementais, laikomais laisvąja ir atvirąja programine įranga, už kuriuos jie nėra atsakingi“ (18 konstatuojamoji dalis).

86. Produktų su skaitmeniniais elementais gamintojai, kurie į savo produktus su skaitmeniniais elementais integruoja FOSS komponentus, taip pat nėra atsakingi už kiekvieno tokio komponento individualią atitiktį KAA, net jei gamintojai prie jų priežiūros prisideda pirminiu kodu.

87. Panašiai vien tai, kad gamintojai integruoja FOSS komponentus į savo (monetizuojamus) produktus su skaitmeniniais elementais, neturi įtakos to FOSS komponento statusui pagal KAA. FOSS komponentų, kurie nėra pateikiami rinkai, techninės priežiūros vykdytojai neturi pareigų kitų subjektų, galinčių integruoti tokius komponentus į savo produktus su skaitmeniniais elementais, atžvilgiu. Ar KAA taikomas konkrečiam FOSS komponentui, priklauso tik nuo to, ar jį skelbiantis fizinis arba juridinis asmuo pateikia jį rinkai.

88. Vis dėlto produktų su skaitmeniniais elementais gamintojai, integruojantys FOSS komponentus, privalo laikytis KAA reikalavimų savo produktų su skaitmeniniais elementais atžvilgiu. Pagal 13 straipsnio 5 dalį jiems taip pat taikoma jų integruojamų FOSS komponentų išsamaus patikrinimo pareiga. Be to, pagal 13 straipsnio 6 dalį jie privalo pranešti apie integruotuose komponentuose nustatytą pažeidžiamumą ir dalytis saugumo pataisomis. Daugiau gairių šia tema pateikta *9.2.1* skirsnyje *„Pranešimų teikimas pirmesnės tiekimo grandies subjektams* ir dalijimasis saugumo pataisomis“.

3.5. **Iliustraciniai scenarijai**

89. Toliau pateikti pavyzdžiai yra visiškai hipotetiniai ir skirti tik įvairiems pirmesniuose skirsniuose paaiškintiems atvejams iliustruoti.

27 pavyzdys. Individualus kūrėjas A sukūrė FOSS. Kūrėjas A paskelbia šią FOSS savo vardu arba naudodamas savo prekių ženklą, tačiau už jos naudojimą neima mokesčio. Programine įranga atvirai dalijamasi ir ji yra laisvai prieinama visiems, kad ją būtų galima pasiekti, naudoti, keisti ir platinti. Kūrėjas A taip pat pateikia nuorodą į platformą savanoriškoms aukoms rinkti.

Įmonės B, C ir D integruoja šią FOSS į savo produktus su skaitmeniniais elementais. Siekdamos prisidėti prie nuolatinės priežiūros, įmonės B, C ir D savanoriškai aukoja kūrėjui A. Šios aukos suteikia kūrėjui A galimybę toliau aktyviai prižiūrėti projektą.

Ši FOSS nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA. Kūrėjas A neturi pareigų pagal KAA. Įmonės B, C ir D, integruodamos šią FOSS į savo produktus su skaitmeniniais elementais, turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

28 pavyzdys. Pelno nesiekiantis fondas F skelbia FOSS komponentą, skirtą integruoti į kitus komercinius produktus su skaitmeniniais elementais. Fondas F įsipareigoja nuolat teikti paramą šiai FOSS, kad užtikrintų jos gyvybingumą ir naudojimą. Įmonės A, B ir C integruoja šią FOSS į savo produktus su skaitmeniniais elementais. Įmonės A ir B savanoriškai skiria dalį savo kūrėjų darbo laiko fondo F FOSS projektams, įskaitant šią FOSS, plėtoti ir prižiūrėti.

Kadangi fondas F yra pelno nesiekiantis subjektas, įsteigtas taip, kad visos jo pajamos, atskaičius išlaidas, būtų naudojamos ne pelno tikslams, FOSS nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA. Fondas F yra FOSS valdytojas ir jam taikomos atitinkamos 24 straipsnyje nustatytos pareigos. Įmonės A, B ir C, integruodamos šią FOSS į savo produktus su skaitmeniniais elementais, turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

29 pavyzdys. Įmonė A sukūrė FOSS komponentą, skirtą integruoti į jos pačios produktus su skaitmeniniais elementais. Ji taip pat atskirai skelbia šią FOSS savo vardu arba naudodama savo prekių ženklą ir aktyviai ją prižiūri. Tačiau ji neima mokesčio už jos naudojimą ir jos nemonetizuoja kitais būdais. Įmonės B, C ir D integruoja šią FOSS į savo produktus su skaitmeniniais elementais ir savanoriškai skiria dalį savo kūrėjų darbo laiko jos priežiūrai.

Ši FOSS nelaikoma pateikta rinkai, kaip tai suprantama pagal KAA. Įmonė A nėra jos gamintoja, tačiau yra jos valdytoja. Įmonės B, C ir D, integruodamos FOSS į savo produktus su skaitmeniniais elementais, turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

30 pavyzdys. Įmonė A skelbia FOSS savo vardu arba naudodama savo prekių ženklą ir siūlo mokamą jos versiją, kuri apima tam tikrus papildomus pranašumus, pavyzdžiui, techninę pagalbą arba veikimo optimizavimą. Įmonėse B, C ir D dirbantys kūrėjai prisideda prie FOSS priežiūros, tačiau FOSS ir toliau kontroliuoja įmonė A.

Įmonė A laikoma šios FOSS gamintoja ([15]). Įmonėms B, C ir D šios konkrečios FOSS atžvilgiu netaikomos pareigos pagal KAA. Jeigu jos integruoja šią FOSS į savo produktus su skaitmeniniais elementais, jos privalo atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

31 pavyzdys. Įmonė A skelbia FOSS savo vardu arba naudodama savo prekių ženklą ir nuolat atlieka jos priežiūrą, kad būtų užtikrintas ilgalaikis jos gyvybingumas ir kad šią programinę įrangą būtų galima integruoti į kitų įmonių produktus su skaitmeniniais elementais. Įmonė A neima mokesčio už jos naudojimą, netvarko asmens duomenų, kuriuos renka naudodama produktą su skaitmeniniais elementais, ir neparduoda su FOSS skelbimu susijusių palaikymo paslaugų.

Įmonė B prisideda programiniu kodu ir skiria joje dirbančių kūrėjų darbo laiko FOSS priežiūrai, tačiau komerciškai jos neplatina. Įmonė B techninės pagalbos paslaugas teikia nepriklausomai nuo FOSS platinimo. Įmonė A laikoma šios FOSS valdytoja, o įmonė B šios FOSS atžvilgiu pagal KAA neturi jokių pareigų.

32 pavyzdys. FOSS komponentą skelbia pelno nesiekiantis subjektas, įsteigtas taip, kad būtų užtikrinta, jog visos pajamos, atskaičius išlaidas, būtų naudojamos ne pelno tikslams. Šis subjektas nuolat teikia paramą, kad užtikrintų ilgalaikį projekto gyvybingumą. Priežiūra finansuojama viešosiomis lėšomis, pavyzdžiui, mokslinių tyrimų dotacijomis. Papildomi patobulinimai, įskaitant naujas funkcijas, finansuojami iš aukų ir pagal konkrečius projektus, vykdomus bendradarbiaujant su gamintojais, kurie integruoja šią FOSS į savo produktus su skaitmeniniais elementais. Tokios funkcijos įtraukiamos į FOSS programinio kodo bazę.

FOSS skelbiantis pelno nesiekiantis subjektas laikomas to FOSS komponento valdytoju. Gamintojas, prisidėjęs prie tam tikrų funkcijų kūrimo, netampa to FOSS komponento gamintoju. Kai gamintojas tą FOSS komponentą integruoja į savo produktą su skaitmeniniais elementais, jis turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

33 pavyzdys. Pelno nesiekiantis subjektas, įsteigtas taip, kad būtų užtikrinta, jog visos pajamos, atskaičius išlaidas, būtų naudojamos ne pelno tikslams, skelbia FOSS programinės įrangos kūrimo priemonių rinkinį (angl. software development kit*, toliau – SDK) ir užtikrina nuolatinę jo priežiūrą. SDK yra atvirai dalijamasi ir jis yra laisvai prieinamas visiems, kad jį būtų galima pasiekti, naudoti, keisti ir platinti. Finansavimas teikiamas iš pelno nesiekiančiam subjektui mokamų narystės mokesčių, o organizacijose narėse dirbantys kūrėjai prie SDK kūrimo prisideda programiniu kodu ir kitais ištekliais. Gamintojai naudoja SDK kaip komponentą kitiems produktams su skaitmeniniais elementais kurti.*

Pelno nesiekiantis subjektas, kuris skelbia tą SDK, yra jo valdytojas. Fondo nariai nėra atsakingi už SDK atitiktį KAA. Kai gamintojai naudoja SDK savo produktui su skaitmeniniais elementais kurti, jie turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

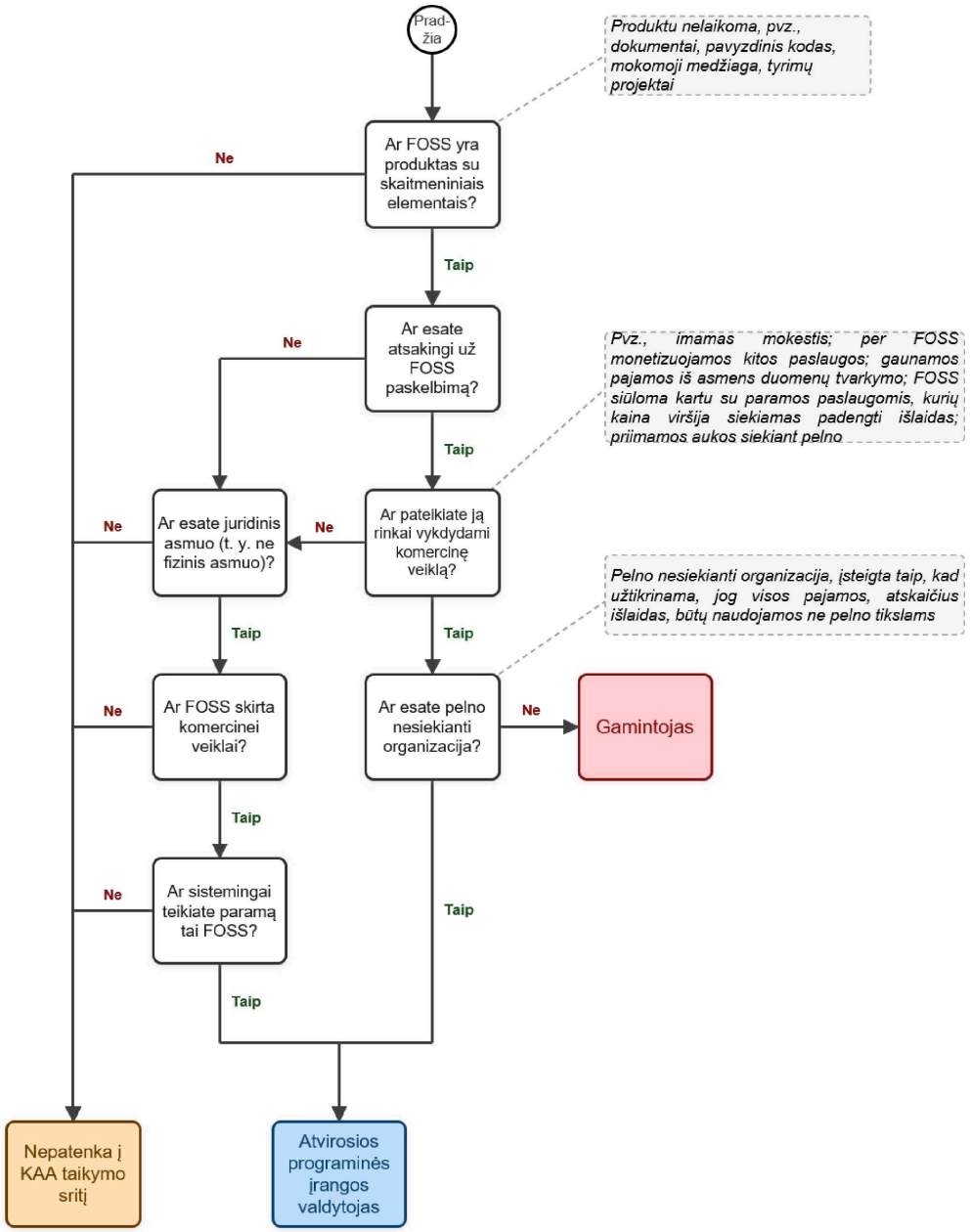
34 pavyzdys. Individualus kūrėjas paskelbia FOSS biblioteką viešoje tam tikrai programavimo kalbai skirtoje paketų saugykloje ir aktyviai ją prižiūri. Paketo dokumentuose kūrėjas pateikia nuorodą aukoms rinkti. Gamintojas tą biblioteką nemokamai parsisiunčia iš saugyklos ir integruoja ją į savo produktą su skaitmeniniais elementais.

Individualiam kūrėjui ir paketų saugyklai netaikomos jokios pareigos pagal KAA. Biblioteką integruojantis gamintojas turi atlikti išsamų patikrinimą pagal 13 straipsnio 5 dalį.

([15]) Išskyrus atvejį, kai įmonė A yra pelno nesiekiantis subjektas, įsteigtas taip, kad būtų užtikrinta, jog visos pajamos, atskaičius išlaidas, būtų naudojamos ne pelno tikslams; tokiu atveju ji būtų šios FOSS valdytoja.

1 pav

Stilizuota KAA taikymo laisvajai ir atvirajai programinei įrangai schema



4. ESMINIAI PAKEITIMAI IR ATSARGINĖS DALYS

90. KAA 3 straipsnio 30 punkte „esminis pakeitimas“ apibrėžiamas kaip produkto su skaitmeniniais elementais pakeitimas po jo pateikimo rinkai, kuris i) daro poveikį produkto su skaitmeniniais elementais atitikčiai I priedo I dalyje nustatytiems esminiams reikalavimams arba ii) dėl kurio pasikeičia numatytoji paskirtis, pagal kurią buvo įvertintas produktas su skaitmeniniais elementais.

91. Esminio pakeitimo samprata yra svarbi nustatant pagal KAA taikomas pareigas įvairiais atvejais, įskaitant šiuos:

a) pagal 21 straipsnį importuotojas arba platintojas, kuris atlieka jau rinkai pateikto produkto su skaitmeniniais elementais esminį pakeitimą, laikomas jo gamintoju;

b) pagal 22 straipsnį bet kuris fizinis ar juridinis asmuo, kuris atlieka produkto su skaitmeniniais elementais esminį pakeitimą ir tiekia jį rinkai, laikomas jo gamintoju;

c) pagal 69 straipsnio 2 dalį, bet kuris fizinis ar juridinis asmuo, kuris po 2027 m. gruodžio 11 d. atlieka anksčiau nei 2027 m. gruodžio 11 d. rinkai pateikto produkto su skaitmeniniais elementais esminį pakeitimą ir pateikia jį rinkai, laikomas jo gamintoju;

d) produktų su skaitmeniniais elementais, pateiktų rinkai po 2027 m. gruodžio 11 d., gamintojams – siekiant nustatyti, ar dėl po tos datos atliktų pakeitimų produktui su skaitmeniniais elementais turi būti taikoma nauja atitikties vertinimo procedūra, visų pirma atsižvelgiant į iteracinį programinės įrangos kūrimo pobūdį.

92. Todėl svarbu pateikti gaires, kurios padėtų ekonominės veiklos vykdytojams suprasti, kada aparatinės ar programinės įrangos pakeitimai laikomi esminiais pakeitimais.

4.1. **Fizinis taisymas**

93. Kaip nurodyta KAA 42 konstatuojamojoje dalyje, „jei produktui su skaitmeniniais elementais taikomas atnaujinimas, techninė priežiūra ir taisymas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2024/1781 2 straipsnio 18, 19 ir 20 punktuose, tai nebūtinai reiškia esminį produkto pakeitimą, pavyzdžiui, jei numatytoji paskirtis nepasikeičia ir funkcijos bei rizikos lygis lieka nepakitę. Tačiau gamintojo atliekamas produkto su skaitmeniniais elementais atnaujinimas gali reikšti produkto projektavimo ir kūrimo pokyčius, todėl gali turėti įtakos jo numatytajai paskirčiai ir atitikčiai šiame reglamente nustatytiems reikalavimams“. Tai atitinka Mėlynojo vadovo 2.1 skirsnį, kuriame primenama, kad „[g]aminys, kuris buvo iš esmės pakeistas arba perdirbtas po to, kai buvo pradėtas naudoti, turi būti laikomas nauju gaminiu, jeigu: i) jo pirminės eksploatacinės savybės, paskirtis ar tipas yra pakeisti, tačiau tai nebuvo numatyta pradiniame rizikos vertinime; ii) dėl pakeitimo pakito pavojaus pobūdis arba padidėjo rizikos lygis atsižvelgiant į atitinkamus Sąjungos derinamuosius teisės aktus ir iii) gaminys tiekiamas rinkai (arba pradedamas naudoti, jei tai patenka į taikytinų teisės aktų taikymo sritį). Tai reikia įvertinti kiekvienu konkrečiu atveju, visų pirma atsižvelgiant į atitinkamų teisės aktų tikslą ir kokios rūšies gaminiams jie taikomi.“

94. Atnaujinimo, techninės priežiūros ar taisymo veiksmai, kuriais fiziškai pakeičiami rinkai jau pateikti produktai su skaitmeniniais elementais, nebūtinai laikomi esminiais pakeitimais. Todėl kiekvienu konkrečiu atveju turėtų būti įvertinta, ar toks fizinis pakeitimas daro poveikį produkto su skaitmeniniais elementais atitikčiai I priedo I dalyje nustatytiems esminiams reikalavimams arba lemia produkto numatytosios paskirties, kuri buvo įtraukta į kibernetinio saugumo rizikos vertinimą, pasikeitimą.

95. Defektų turinčių dalių arba susidėvėjusių elementų pakeitimas geresnėmis eksploatacinėmis savybėmis pasižyminčiomis dalimis (pvz., dėl technikos pažangos arba dėl to, kad senoji dalis nebegaminama) savaime nereiškia, kad pataisytas produktas su skaitmeniniais elementais yra iš esmės pakeistas. Esminiu pakeitimu tai laikoma tik tuo atveju, jei eksploatacinių savybių pokytis arba pataisyto produkto su skaitmeniniais elementais veikimo būdas i) daro poveikį jo atitikčiai esminiams reikalavimams arba ii) lemia numatytosios paskirties pokytį, kuris nebuvo numatytas rizikos vertinime.

35 pavyzdys. Kompiuterių serverio gamintojas atlieka taisymo darbus ir sugedusią RAM pakeičia nauja, geresnių eksploatacinių savybių RAM. Tai nedaro poveikio serverio atitikčiai esminiams reikalavimams. Serverio eksploatacinės savybės pagerėja, tačiau jį toliau eksploatuojant neperžengiamos serverio numatytosios paskirties, į kurią buvo atsižvelgta atliekant kibernetinio saugumo rizikos vertinimą, ribos. Serveris nelaikomas iš esmės pakeistu.

4.2. **Atsarginės dalys**

96. KAA 2 straipsnio 6 dalyje nustatyta, kad atsarginėms dalims, skirtoms identiškiems komponentams pakeisti ir pagamintoms pagal tas pačias specifikacijas kaip ir tie komponentai, KAA netaikomas. 29 konstatuojamojoje dalyje taip pat nurodyta, kad ši išimtis taikoma tiek produktų su skaitmeniniais elementais, kurie buvo tiekiami rinkai iki KAA taikymo pradžios, atsarginėms dalims, tiek atsarginėms dalims, dėl kurių jau atlikta reglamente nustatyta atitikties vertinimo procedūra.

97. KAA 2 straipsnio 6 dalyje nustatyta išimtis turėtų būti suprantama kaip taikoma tik tais atvejais, kai atsarginė dalis konkrečiai tiekiama siekiant pataisyti rinkai jau pateiktą produktą su skaitmeniniais elementais arba padidinti jo patvarumą (nepriklausomai nuo to, ar jis rinkai pateiktas anksčiau nei 2027 m. gruodžio 11 d., ar po šios datos). Kai produktas su skaitmeniniais elementais tiekiamas kaip atskiras produktas, nesiejant jo su jau egzistuojančio produkto su skaitmeniniais elementais priežiūra ar taisymu, jis laikomas pateiktu rinkai, kaip tai suprantama pagal KAA, ir neturėtų būti laikomas atsargine dalimi, patenkančia į 2 straipsnio 6 dalies taikymo sritį. Techninės priežiūros ar taisymo paskirtis turėtų būti aiški iš tiekimo aplinkybių, pavyzdžiui, kai konkretus produktas su skaitmeniniais elementais ar produktų grupė nurodomi užsakyme ar komerciniame pasiūlyme arba kai tiekiama garantinio aptarnavimo ar techninės priežiūros kanalais. Tai patvirtinantys įrodymai taip pat turėtų būti saugomi ir prireikus pateikiami rinkos priežiūros institucijoms. Vien tai, kad produktas su skaitmeniniais elementais techniškai galėtų būti naudojamas komponentui pakeisti, savaime nėra pakankama priežastis taikyti šią išimtį, jeigu nėra minėtų aplinkybių.

98. Atitinkamai, kai atsarginė dalis yra identiška komponentui, kuris jau yra įtrauktas į produktą su skaitmeniniais elementais, pateiktą rinkai arba iki KAA taikymo pradžios datos, arba laikantis KAA reikalavimų, pačiai tai atsarginei daliai KAA netaikomas.

99. Vertinant, ar atsarginė dalis turėtų būti laikoma identiška komponentui, daugiausia dėmesio turėtų būti skiriama jo funkcinei paskirčiai produkte su skaitmeniniais elementais ir toms savybėms, kurios gali būti svarbios kibernetiniam saugumui. Nors kiekvienu atveju būtinas individualus vertinimas, skirtumai, kurie neturi įtakos komponento saugumo savybėms ar jo kibernetinio saugumo rizikos profiliui, savaime nereiškia, kad tokia atsarginė dalis nepatenka į KAA 2 straipsnio 6 dalies taikymo sritį.

100. Kita vertus, komponento kibernetiniam saugumui svarbių savybių, pavyzdžiui, algoritmų, protokolų, kriptografinių mechanizmų, prieigos kontrolės funkcijų ar kitų su saugumu susijusių savybių, skirtumai gali reikšti, kad naujoji dalis negali būti laikoma identiška komponentui, kuriam pakeisti ji skirta.

101. Kai atsarginė dalis nėra identiška pirminiam komponentui, tokia atsarginė dalis pati savaime laikoma produktu su skaitmeniniais elementais, todėl jai taikomas KAA. Tokiais atvejais atitiktis esminiams reikalavimams turi būti vertinama atsižvelgiant į keičiamo komponento numatytąją paskirtį. Ypač svarbi yra keičiamo komponento funkcija užtikrinti suderinamumą ar sąveikumą su esamu produktu su skaitmeniniais elementais, įskaitant atvejus, kai tas produktas su skaitmeniniais elementais buvo pateiktas rinkai dar iki KAA taikymo pradžios. Kai dėl tokios numatytosios paskirties ar techninių apribojimų pagrįstai neįmanoma įvykdyti tam tikrų esminių reikalavimų, gamintojas turi tai atspindėti kibernetinio saugumo rizikos vertinime ir įgyvendinti tinkamas alternatyvias ar kompensacines rizikos mažinimo priemones, kad nebūtų pakenkta produkto su skaitmeniniais elementais saugumui. Kaip aptarta ir *2.6* skirsnyje „*Sudėtingos sistemos*“, tiek techniniai dokumentai, tiek naudotojui skirta informacija ir instrukcijos atlieka svarbų vaidmenį skaidriai aprašant nustatytus apribojimus, su jais susijusią kibernetinio saugumo riziką ir įgyvendintas rizikos mažinimo priemones. Kaip paaiškinta *4.1* skirsnyje „*Fizinis taisymas*“, defektų turinčių dalių ar susidėvėjusių elementų pakeitimas geresnių eksploatacinių savybių dalimis savaime nereiškia, kad pataisytas produktas su skaitmeniniais elementais yra iš esmės pakeistas.

36 pavyzdys. Gamintojas pateikė ES rinkai susietuosius valdiklius. Vienu atveju valdiklis buvo pateiktas rinkai 2026 m., iki KAA taikymo pradžios datos. Kitu atveju valdiklis buvo pateiktas rinkai 2028 m., laikantis KAA reikalavimų. 2028 m. abiejų tipų valdikliuose sugenda skaitmeninio ryšio modulis. Gamintojas kaip atsarginę dalį pateikia pakaitinį modulį, kuris yra identiškas pirminiam ir pagamintas pagal tas pačias specifikacijas.

Abiem atvejais pakaitiniam moduliui taikoma 2 straipsnio 6 dalyje nustatyta išimtis. Pačiai atsarginei daliai KAA netaikomas, nors ji ir yra produktas su skaitmeniniais elementais, nes ja pakeičiamas identiškas produkto su skaitmeniniais elementais komponentas. Toks taisymas nelaikomas esminiu produkto su skaitmeniniais elementais pakeitimu.

37 pavyzdys. Gamintojas 2026 m., iki KAA taikymo pradžios datos, pateikė ES rinkai susietąjį pramoninį valdiklį. 2028 m. tame valdiklyje sugenda ryšio lustas. Kadangi gamintojas šio lusto nebegamina, jis kaip atsarginę dalį pateikia naujesnį analogiškas funkcijas atliekantį lustą, tačiau jame taikomas kitoks kriptografinio įdiegimo būdas ir atnaujintas saugaus paleidimo mechanizmas, kad būtų išlaikytas suderinamumas ir užtikrintas tolesnis veikimas.

Šiuo atveju pakaitinis lustas negali būti laikomas identišku, nes kriptografinio įdiegimo ir saugaus paleidimo mechanizmo skirtumai turi įtakos lusto kibernetinio saugumo savybėms. Todėl jam netaikoma 2 straipsnio 6 dalyje nustatyta išimtis ir jis laikomas produktu su skaitmeniniais elementais, kuriam taikomas KAA. Pakaitinės dalies atitiktis reikalavimams turi būti vertinama atsižvelgiant į jos numatytąją paskirtį, įskaitant jos vaidmenį užtikrinant sąveikumą su produktu su skaitmeniniais elementais, pateiktu rinkai iki KAA taikymo pradžios.

38 pavyzdys. Gamintojas 2028 m., laikydamasis KAA reikalavimų, pateikia rinkai išmaniojo pastato valdiklį. 2029 m. tame valdiklyje sugenda belaidžio ryšio modulis. Kadangi gamintojas šio modulio nebegamina, jis kaip atsarginę dalį pateikia naują modulį, kuris atlieka tą pačią funkciją, naudodamasis tais pačiais ryšio protokolais ir saugumo mechanizmais, tačiau yra pagrįstas kitu lustų rinkiniu ir turi atnaujintą aparatinę programinę įrangą, nekeičiančią savybių, kurios gali būti svarbios kibernetiniam saugumui.

Šiuo atveju pakaitinis modulis gali būti laikomas identišku, todėl jam taikoma 2 straipsnio 6 dalyje nustatyta išimtis ir netaikomas KAA.

102. Atsarginėms dalims išimtis taikoma nepriklausomai nuo to, ar atsargine dalimi pakeičiamas produkto su skaitmeniniais elementais komponentas, ar visas produktas su skaitmeniniais elementais, kuris pats yra didesnio produkto dalis, įskaitant atvejus, kai toks didesnis produktas su skaitmeniniais elementais sudarytas iš kelių integruotų komponentų, su sąlyga, kad pakaitinė dalis yra konkrečiai tiekiama kaip atsarginė dalis, kaip paaiškinta pirmesnėse dalyse.

39 pavyzdys. 2027 m. gamintojas pateikia rinkai pramoninę automatizavimo sistemą, kurios vienas iš komponentų yra programuojamasis loginis valdiklis (PLC). 2031 m. sugenda PLC centrinis procesorius (CPU). Gamintojas siūlo du taisymo variantus: i) pateikti pakaitinį CPU, kuris gali būti laikomas identišku iš pradžių įmontuotam CPU, ii) pateikti visą pakaitinį PLC, kuris gali būti laikomas identišku iš pradžių įmontuotam PLC. Abiem atvejais pakaitinė dalis tiekiama gamintojo garantinio aptarnavimo kanalu kaip atsarginė dalis, o pramoninė automatizavimo sistema, kuriai ta pakaitinė dalis skirta, yra aiškiai identifikuota. Abiem atvejais pakaitinei daliai taikoma 2 straipsnio 6 dalyje nustatyta išimtis, neatsižvelgiant į tai, ar keičiamas PLC komponentas, ar visas PLC.

4.3. **Programinės įrangos naujinimai kaip esminiai pakeitimai**

103. Programinės įrangos kūrimas yra iteracinio pobūdžio, todėl rinkai jau pateikti programinės įrangos produktai su skaitmeniniais elementais yra dažnai ir nuolat atnaujinami. Atsižvelgiant į tai, naudinga pateikti išsamesnių gairių, padedančių nustatyti, kada programinė įranga turi būti laikoma iš esmės pakeista. Tokios gairės visų pirma skirtos padėti programinės įrangos produktų su skaitmeniniais elementais gamintojams, kurie keičia savo pačių produktus, nustatyti, ar tokie pakeitimai laikytini esminiais pakeitimais.

104. 39 konstatuojamojoje dalyje nurodyta, kad produktas su skaitmeniniais elementais laikomas iš esmės pakeistu, kai dėl pakeitimo pakinta kibernetinio saugumo rizikos lygis ir kai gamintojas į tokią pasikeitusią ar papildomą riziką nėra atsižvelgęs atlikdamas rizikos vertinimą, taigi ir įgyvendindamas esminius reikalavimus. Todėl gamintojas kiekvienu konkrečiu atveju turėtų įvertinti, ar programinės įrangos naujinys kelia naują arba didesnę kibernetinio saugumo riziką ir ar į tokią riziką jau atsižvelgta atliekant rizikos vertinimą.

105. Kai gamintojas produkte su skaitmeniniais elementais įdiegia naujų funkcijų, dėl kurių pasikeičia viso produkto numatytoji paskirtis, tikėtina, kad gamintojas į tokius pakeitimus nėra atsižvelgęs atlikdamas rizikos vertinimą. Tokiomis aplinkybėmis pakeitimas paprastai būtų laikomas esminiu pakeitimu.

40 pavyzdys. Gamintojas pateikia rinkai informacinį skydelį, kuriame renkami duomenys iš įrenginių ir rodomos tendencijos bei įspėjimai, tačiau kuris negali tų įrenginių valdyti. Vėliau gamintojas sukuria naują to informacinio skydelio versiją ir įdiegia funkcijas, leidžiančias valdyti įrenginius, be kita ko, reguliuoti jų veikimo parametrus ir iš naujo paleisti įrenginius po gedimų. Dėl šių pakeitimų informacinio skydelio numatytoji paskirtis išplečiama už rizikos vertinime numatytų ribų: iš padėties stebėsenai skirtos priemonės jis tampa produktu su skaitmeniniais elementais, skirtu kitų įrenginių veikimui valdyti. Todėl informacinis skydelis yra iš esmės pakeistas.

41 pavyzdys. Gamintojas pateikia rinkai vartotojams skirtą taikomąją programinę įrangą, kurios paskirtis – tvarkyti ir rodyti asmens duomenis, pavyzdžiui, e. laiškus, žinutes ar dokumentus, ir suteikti pagrindines paieškos bei filtravimo funkcijas. Vėliau gamintojas pateikia naujinį, kuriuo taikomajai programai suteikiama geba automatiškai analizuoti naudotojo turinį, kad būtų sudaromi elgesio profiliai ir be naudotojo įsikišimo priimami automatizuoti sprendimai, turintys įtakos turinio prioritetų nustatymui, jo slėpimui ar rekomendavimui. Dėl šio pakeitimo programinės įrangos numatytoji paskirtis pasikeičia: iš naudotojo valdomos informacijos tvarkymo priemonės ji tampa automatizuoto sprendimų priėmimo sistema, kuri nebuvo numatyta atliekant rizikos vertinimą. Taigi taikomoji programa yra iš esmės pakeista.

106. Tačiau kartu gali būti taip, kad gamintojas laipsniškai įdiegia naujas funkcijas, kurios jau įtrauktos į jo rizikos vertinimą arba kurios savaime nekeičia produkto su skaitmeniniais elementais kibernetinio saugumo rizikos profilio. Taip gali būti, pavyzdžiui, kai gamintojas iš anksto numatė tokių funkcijų kūrimą, jau apibūdino ir įvertino su jomis susijusią riziką ir įgyvendino tinkamas rizikos mažinimo priemones, kad būtų užtikrinta nuolatinė atitiktis esminiams reikalavimams. Taip gali būti ir tais atvejais, kai naujomis funkcijomis neįgyvendinami pakeitimai, dėl kurių kiltų nauja ar padidėtų esama rizika. Todėl tokio pobūdžio naujiniai neturėtų būti laikomi esminiais pakeitimais, nes jie nedidina kibernetinio saugumo rizikos ir dėl to nekeičia esminių reikalavimų įgyvendinimo.

42 pavyzdys. Pranešimų siuntimo taikomoji programa iš pradžių išleidžiama tik su individualių pranešimų siuntimo funkcija. Gamintojo atliktame rizikos vertinime numatyta, kad vėliau bus įdiegta grupinių pranešimų siuntimo funkcija, įskaitant, pavyzdžiui, didesnį pranešimų maršruto parinkimo sudėtingumą. Vėliau pateikiamu naujiniu gamintojas prideda grupinių pokalbių funkciją kartu su administratoriui skirtomis valdymo priemonėmis ir moderavimo priemonėmis, kurios jau buvo numatytos ir įvertintos pradiniame projekte. Naujiniu įdiegiamos funkcijos, patenkančios į pirminės numatytosios paskirties ir rizikos vertinimo aprėptį. Taigi pranešimų siuntimo taikomoji programa nėra iš esmės pakeista.

43 pavyzdys. Gamybos stebėsenos sistema pateikiama rinkai su įjungtais tik skaityti skirtais informaciniais skydeliais, o automatinio valdymo funkcijos yra numatytos sistemos architektūroje, tačiau lieka išjungtos. Gamintojo atliktame rizikos vertinime aiškiai numatytas būsimas automatinio valdymo ciklų aktyvavimas, įskaitant su uždarojo ciklo valdymu susijusią kibernetinio saugumo riziką, taip pat apsaugos priemones, kaip antai operatoriui skirtus valdymo perėmimo mechanizmus ir gedimo atveju saugias būsenas. Vėlesniu naujiniu gamintojas įjungia automatinio valdymo funkcijas ir aktyvuoja apsaugos priemones taip, kaip buvo numatyta pirminiame vertinime. Taigi gamybos stebėsenos sistema nėra iš esmės pakeista.

107. Kita vertus, net ribotos apimties ar iš pažiūros nedidelės naujos funkcijos gali sukelti reikšmingą kibernetinio saugumo riziką, darančią poveikį atitikčiai esminiams reikalavimams. Todėl vertinant, ar pakeitimas yra esminis, reikėtų atsižvelgti ne į pakeitimo mastą ar sudėtingumą, o į jo galimą neigiamą poveikį produkto su skaitmeniniais elementais kibernetinio saugumo rizikos profiliui ir atitinkamai esminių reikalavimų įgyvendinimui.

44 pavyzdys. Gamintojas pateikia taikomosios programinės įrangos naujinį, kuriuo pridedama funkcija „prisiminti mane“ arba nuolatinio prisijungimo funkcija, vietoje išsaugant prieigos raktus naudotojo patogumui padidinti. Nors ši funkcija yra ribotos apimties, ji sukelia naują riziką, susijusią su prieigos raktų vagyste, neteisėta prieiga ir seanso užgrobimu, į kurią nebuvo atsižvelgta rizikos vertinime. Taigi naujinys daro poveikį atitikčiai esminiams reikalavimams. Taikomoji programinė įranga yra iš esmės pakeista.

45 pavyzdys. Gamintojas esamą programinės įrangos produktą su skaitmeniniais elementais papildo nauja registravimo ir diagnostikos funkcija, leidžiančia eksportuoti išsamius sistemos žurnalus trikčių šalinimo tikslais. Nors ši funkcija gali atrodyti nereikšminga, dėl jos renkami ir nešifruotu formatu saugomi neskelbtini veiklos duomenys, todėl kyla duomenų atskleidimo rizika, kuri anksčiau nebuvo įvertinta ar sumažinta. Todėl šis pakeitimas gali daryti reikšmingą poveikį produkto su skaitmeniniais elementais kibernetinio saugumo rizikos profiliui. Programinės įrangos produktas su skaitmeniniais elementais yra iš esmės pakeistas.

108. Pagal KAA 39 konstatuojamąją dalį saugumo naujiniai paprastai nelaikytini esminiais pakeitimais, nes jų pagrindinis tikslas yra sumažinti su produktu su skaitmeniniais elementais susijusios kibernetinio saugumo rizikos lygį. Todėl saugumo naujinys, kuris nekeičia to produkto numatytosios paskirties ir nesukelia naujos kibernetinio saugumo rizikos, neturėtų būti laikomas esminiu pakeitimu, net jei tokiu naujiniu atliekami reikšmingi techniniai pakeitimai. Tai taip pat apima atvejus, kai tam tikros funkcijos pakeičiamos ar apribojamos vien tam, kad būtų sumažintas nustatyto pažeidžiamumo poveikis ir užtikrinta nuolatinė atitiktis esminiams reikalavimams.

46 pavyzdys. Gamintojas įdiegia saugumo naujinį, kad pašalintų produkto su skaitmeniniais elementais programinio kodo bazės pažeidžiamumą, ištaisydamas įvesties duomenų tikrinimo klaidą, dėl kurios galėtų įvykti buferio perpildymas, arba loginę klaidą, leidžiančią apeiti tapatumo nustatymą dėl netinkamo seanso prieigos rakto tikrinimo. Naujiniu pakeičiamas vidinis programinės įrangos įdiegimo būdas, nedarant poveikio to produkto numatytajai paskirčiai ir nesukuriant naujų rizikos poveikio galimybių. Toks naujinys skirtas tik kibernetinio saugumo rizikai sumažinti. Saugumo naujinys neturėtų būti laikomas esminiu pakeitimu.

47 pavyzdys. Gamintojas pateikia saugumo naujinį, kuriuo sustiprinamos esamos saugumo konfigūracijos, pavyzdžiui, sugriežtinamos užkardos taisyklės, išjungiami nenaudojami tinklo prievadai, pakeičiamos numatytųjų administratoriaus slaptažodžių taisyklės arba daugiaveiksnis tapatumo nustatymas padaromas privalomas tais atvejais, kai tokia funkcija jau yra prieinama arba numatyta. Nors naujinys gali turėti įtakos tam, kaip naudotojai konfigūruoja produktą su skaitmeniniais elementais arba gauna prieigą prie jo, jis nekeičia produkto numatytosios paskirties ir yra skirtas tik jo saugumo būklei pagerinti. Saugumo naujinys neturėtų būti laikomas esminiu pakeitimu.

48 pavyzdys. Gamintojas pateikia rinkai programinės įrangos produktą su skaitmeniniais elementais, kuriame ryšiams apsaugoti naudojama konfigūruojama šifravimo sistema, palaikanti kelis kriptografinius algoritmus ir skirtingus raktų ilgius, kaip aprašyta produkto techniniuose dokumentuose ir rizikos vertinime. Rizikos vertinimas apima visas produkte su skaitmeniniais elementais numatytas kriptografines parinktis ir jame numatomas būsimas tam tikrų algoritmų naudojimo nutraukimas. Rizikos vertinime taip pat numatytos rizikos mažinimo priemonės, pavyzdžiui, kriptografinis lankstumas, vidinis raktų valdymas ir suderinamumo bandymai. Atsižvelgdamas į naujas kriptografijos srities gaires, gamintojas įdiegia saugumo naujinį, kuriuo išjungiamas nebenaudotinas algoritmas ir aktyvuojama tvirtesnė, jau palaikoma alternatyva, nesukuriant naujos išorinės priklausomybės ir nekeičiant duomenų srautų. Kadangi saugumo naujiniu įgyvendinama saugumo priemonė, kuri buvo numatyta ir įvertinta pirminiame projekte, ir jis nesukelia naujos kibernetinio saugumo rizikos, naujinys neturėtų būti laikomas esminiu pakeitimu.

109. Ir, priešingai, saugumo naujinys gali būti laikomas esminiu pakeitimu, kai, nepaisant jo saugumo tikslo, dėl naujinio produkto su skaitmeniniais elementais numatytoji paskirtis pakeičiama labiau, nei buvo numatyta iš pradžių, arba atsiranda nauja ar padidėja esama kibernetinio saugumo rizika. Taip gali būti, pavyzdžiui, kai naujiniu produkto ribos arba priklausomybių struktūra iš esmės pakeičiamos taip, kaip nebuvo numatyta rizikos vertinime, pavyzdžiui, iš esmės pakeičiami duomenų srautai arba pridedamos naujos iš išorės pasiekiamos sąsajos.

49 pavyzdys. Gamintojas pateikia rinkai programinės įrangos produktą su skaitmeniniais elementais, skirtą naudotojo įrenginyje saugomiems duomenims vietoje šifruoti, suteikiant naudotojams galimybę prireikus užšifruoti ir iššifruoti failus. Aptikus šifravimo proceso pažeidžiamumą, gamintojas įdiegia saugumo naujinį, kuriuo pašalinama vietinio šifravimo funkcija ir vietoj jos reikia visus failus įkelti į gamintojo valdomą nuotolinio šifravimo paslaugos sistemą, joje juos saugoti ir apdoroti. Dėl šio pakeitimo produktas su skaitmeniniais elementais nebeatlieka vietinio šifravimo taip, kaip buvo numatyta iš pradžių, o vietoj to veikia kaip nuotolinio šifravimo ir duomenų tvarkymo paslauga. Nors naujinys pateiktas saugumo sumetimais, juo produkto numatytoji paskirtis iš esmės pakeičiama taip, kaip nebuvo numatyta rizikos vertinime, todėl jis laikomas esminiu pakeitimu.

50 pavyzdys. Gamintojas pateikia rinkai programinės įrangos produktą su skaitmeniniais elementais, kuriame ryšiams tarp produkto su skaitmeniniais elementais komponentų apsaugoti naudojamas nusistovėjęs šifravimo protokolas ir viduje valdomas raktų naudojimo ciklas. Reaguodamas į naujai nustatytus kriptografinius trūkumus, gamintojas įdiegia saugumo naujinį, kuriuo esamas šifravimo mechanizmas pakeičiamas kitu protokolu, kuriam būtina naudoti trečiosios šalies valdomą išorinę raktų valdymo paslaugą. Dėl šio pakeitimo iš esmės pakinta produkto su skaitmeniniais elementais priklausomybės šaltiniai ir duomenų srautai – atsiranda naujų išorinių sąsajų ir priklausomybė nuo trečiųjų šalių paslaugų, į kurias nebuvo atsižvelgta rizikos vertinime. Nors naujinys diegiamas saugumo tikslais, jis kelia naują kibernetinio saugumo riziką, todėl yra laikomas esminiu pakeitimu.

110. Kaip nurodyta 104 punkte, tai, ar programinės įrangos naujinys laikytinas esminiu pakeitimu, turėtų būti vertinama kiekvienu konkrečiu atveju. Atlikdami tokį vertinimą gamintojai gali, be kita ko, atsižvelgti į tai, ar programinės įrangos naujinys:

a) sukuria naujų grėsmių vektorių, pavyzdžiui, papildomų sąsajų, ryšio kanalų, vykdymo aplinkų ar išorinių priklausomybių, per kurias galėtų realizuotis grėsmės;

b) sudaro sąlygas naujiems atakų scenarijams, įskaitant, pavyzdžiui, naujus būdus, kuriais galėtų būti realiai įmanoma be leidimo gauti prieigą prie produkto su skaitmeniniais elementais ar jo tvarkomų duomenų, manipuliuoti jais, daryti jiems poveikį arba jais netinkamai naudotis;

c) pakeičia anksčiau nustatytų atakų scenarijų tikimybę, pavyzdžiui, sumažindamas jiems išnaudoti reikalingas pastangas ar kompetenciją, padidindamas nepatikimų subjektų prieigos galimybes arba susilpnindamas esamas apsaugos priemones;

d) pakeičia galimą anksčiau nustatytų atakų scenarijų poveikį, įskaitant, pavyzdžiui, paveikiamų duomenų ar funkcijų apimtį, veiklos, saugos ar ekonominių padarinių sunkumą arba galimybes aptikti incidentą, jį sustabdyti ar po jo atkurti veiklą.

111. Tam tikrais atvejais programinės įrangos naujinys nesukuria naujų grėsmių vektorių, nesudaro sąlygų naujiems atakų scenarijams ir iš esmės nepakeičia anksčiau nustatytų atakų scenarijų tikimybės ar poveikio. Tai gali rodyti, kad dėl naujinio neatsiranda naujos ar didesnės kibernetinio saugumo rizikos, jeigu prielaidos ir rizikos mažinimo priemonės, kuriomis buvo remtasi atliekant rizikos vertinimą, išlieka pagrįstos ir veiksmingos. Todėl tikėtina, kad toks naujinys nelaikytinas esminiu pakeitimu.

112. Kita vertus, dėl programinės įrangos naujinio gali atsirasti naujų grėsmių vektorių, gali būti sudarytos sąlygos naujiems atakų scenarijams arba gali iš esmės pakisti esamų atakų scenarijų tikimybė ar poveikis. Tokiais atvejais gamintojas turėtų iš naujo įvertinti produkto su skaitmeniniais elementais kibernetinio saugumo riziką ir nustatyti, ar tebesilaikoma esminių reikalavimų, įskaitant tai, ar dėl naujinio neatsiranda naujos arba didesnės rizikos, kuri nebuvo numatyta atliekant rizikos vertinimą.

113. Tai, ar programinės įrangos naujinys laikomas esminiu pakeitimu, yra svarbu nustatant, ar taikomos tam tikros KAA nustatytos pareigos, kaip nurodyta 91 punkte. Tačiau, nepriklausomai nuo to, ar naujinys laikomas esminiu pakeitimu, gamintojai ir toliau yra atsakingi už programinės įrangos naujinių ir savo produkto su skaitmeniniais elementais saugumo užtikrinimą jo palaikymo laikotarpiu, laikantis KAA I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų. Be to, nepriklausomai nuo to, ar programinės įrangos naujiniai laikomi esminiais pakeitimais, ar ne, gamintojai pagal 13 straipsnio 7 dalį ir 31 straipsnio 2 dalį privalo užtikrinti, kad rizikos vertinimas ir techniniai dokumentai būtų tikslūs, išsamūs ir nuolat atnaujinami.

4.4. **Esminio pakeitimo pasekmės**

114. Esminio pakeitimo, kurį atlieka ne pirminis jau rinkai pateikto produkto su skaitmeniniais elementais gamintojas, o kitas subjektas, pasekmės reglamentuojamos KAA 21 ir 22 straipsniuose. 21 straipsnis taikomas importuotojams ir platintojams, o 22 straipsnis – bet kuriam fiziniam ar juridiniam asmeniui, kuris nėra gamintojas, importuotojas ar platintojas.

115. Kai esminį pakeitimą atlieka pirminis produkto su skaitmeniniais elementais gamintojas, pasekmių atsiranda dėl KAA 41 konstatuojamojoje dalyje nurodytos visuotinai pripažintos esminio pakeitimo sampratos, kuri išsamiau paaiškinta Mėlynojo vadovo 2.1 skirsnyje. Tame skirsnyje nurodyta, kad produktas, kuris po to, kai buvo pateiktas rinkai, buvo iš esmės pakeistas arba perdirbtas, laikytinas nauju produktu, jeigu buvo pakeistos jo pirminės eksploatacinės savybės, paskirtis ar tipas, pasikeitė pavojaus pobūdis arba padidėjo rizikos lygis ir produktas su skaitmeniniais elementais yra tiekiamas rinkai.

116. Taigi visuotinai pripažinta pasekmė yra ta, kad tais atvejais, kai produkto su skaitmeniniais elementais pakeitimas laikomas esminiu pakeitimu ir pakeistas produktas su skaitmeniniais elementais tiekiamas rinkai, KAA taikymo tikslais jis turi būti laikomas nauju produktu su skaitmeniniais elementais. Todėl iš esmės pakeisto produkto tiekimas rinkai laikomas nauju pateikimu rinkai. Tai taikoma neatsižvelgiant į tai, ar esminį pakeitimą atlieka pirminis gamintojas, ar kitas asmuo. Siekiant užtikrinti, kad KAA būtų vienodai ir proporcingai taikomas įvairių kategorijų subjektams, galintiems atlikti esminį pakeitimą, tolesniuose poskirsniuose aptariamos pareigos, tenkančios esminį pakeitimą atliekančiam asmeniui, kai iš esmės pakeistas produktas su skaitmeniniais elementais pateikiamas rinkai. Pasekmės produkto su skaitmeniniais elementais palaikymo laikotarpiui aptariamos 5 skirsnyje „*Palaikymo laikotarpis*“.

4.4.1. *Esminiai pakeitimai, kuriuos atlieka kitas nei pirminis gamintojas asmuo*

117. Pagal 21 ir 22 straipsnius, kai jau rinkai pateikto produkto su skaitmeniniais elementais esminį pakeitimą atlieka fizinis ar juridinis asmuo, kuris nėra to produkto su skaitmeniniais elementais gamintojas, esminį pakeitimą atliekantis ir pakeistą produktą su skaitmeniniais elementais rinkai tiekiantis asmuo laikomas pakeisto produkto su skaitmeniniais elementais gamintoju, neatsižvelgiant į tai, ar tas asmuo dalyvavo pirminiame to produkto projektavimo ar pateikimo rinkai procese.

118. 22 straipsnyje taip pat patikslinama, kad pakeitimą atliekančiam asmeniui 13 ir 14 straipsniuose nustatytos pareigos taikomos tik tos produkto su skaitmeniniais elementais dalies, kuriai esminis pakeitimas daro poveikį, atžvilgiu, jeigu tas pakeitimas nedaro poveikio viso produkto su skaitmeniniais elementais kibernetiniam saugumui.

119. Kai esminis pakeitimas daro poveikį atitikčiai esminiams reikalavimams, tačiau nedaro neigiamo poveikio viso produkto su skaitmeniniais elementais kibernetiniam saugumui, pakeitimą atliekančiam asmeniui 13 straipsnis (įskaitant pareigą užtikrinti atitiktį esminiams reikalavimams ir atlikti atitikties vertinimo procedūrą) ir 14 straipsnis (pareigos pranešti) taikomi tik tos produkto su skaitmeniniais elementais dalies, kuri yra iš esmės pakeista, atžvilgiu ([16]). Be to, pirminio gamintojo pareigos pagal KAA ir toliau taikomos pirminiam rinkai pateiktam produktui su skaitmeniniais elementais, taip užtikrinant nepakeistų dalių pažeidžiamumo valdymo ir atitikties reikalavimams tęstinumą.

120. Esminio pakeitimo atvejis nepainiotinas su integravimo atvejais, kai asmuo sujungia komponentus (prireikus juos ir pakeisdamas) į naują produktą su skaitmeniniais elementais, kurį pats pateikia rinkai. Tokiais atvejais integruotojas nekeičia kito gamintojo jau rinkai pateikto produkto su skaitmeniniais elementais; priešingai, jis rinkai pateikia savo naują produktą su skaitmeniniais elementais. KAA taikymo tikslais integruotojas yra to naujo produkto su skaitmeniniais elementais gamintojas ir privalo viso produkto su skaitmeniniais elementais atžvilgiu laikytis visų reglamento reikalavimų. Kai gamintojas integruoja komponentus, kuriems taikomas KAA, siekdamas palengvinti savo paties atitikties KAA reikalavimams užtikrinimą, jis gali remtis tų komponentų gamintojų atliktais atitikties užtikrinimo veiksmais.

51 pavyzdys. Įmonė iš tiekėjų, kurie yra trečiosios šalys, įsigyja standartinius rinkoje parduodamus mikrovaldiklių modulius ir junglumo komponentus, sukuria nuosavybinę aparatinę programinę įrangą bei jutiklių rinkinį, juos sujungia į susietąjį žemės ūkio stebėsenos produktą su skaitmeniniais elementais ir jį pateikia rinkai savo vardu. Nors įmonė pakeitė pagrindinius mikrovaldiklių modulius ir sujungė juos su kitais komponentais, ji neatlieka jau rinkai pateikto produkto su skaitmeniniais elementais esminio pakeitimo; priešingai, ji pateikia rinkai naują produktą su skaitmeniniais elementais. KAA taikymo tikslais įmonė yra šio žemės ūkio stebėsenos produkto gamintoja ir privalo laikytis reglamento reikalavimų viso žemės ūkio stebėsenos produkto atžvilgiu.

([16]) Vadovaujantis Mėlynojo vadovo 2.1 skirsniu, „[n]ebūtina kartoti bandymų ir parengti naujų dokumentų dėl tų dalykų, kurie iš dalies pakeitus gaminį nepasikeitė. Įrodyti, kad ne visus techniniuose dokumentuose pateiktus duomenis būtina atnaujinti, yra gaminį pakeitusio arba užsakiusio jį pakeisti fizinio arba juridinio asmens pareiga. Fizinis arba juridinis asmuo, kuris atlieka pakeitimą arba paveda pakeisti gaminį, atsako už pakeisto gaminio atitiktį ir parengia atitikties deklaraciją, net jei jis naudoja esamus bandymus ir techninius dokumentus.“

121. Kai esminis pakeitimas, kurį atlieka kitas nei pirminis gamintojas asmuo, daro neigiamą poveikį viso produkto su skaitmeniniais elementais kibernetiniam saugumui, pavyzdžiui, dėl to, kad pakeitimas nebėra skirtas konkrečiam komponentui ar posistemiui arba jais neapsiriboja, pakeistas rinkai tiekiamas produktas su skaitmeniniais elementais turėtų būti laikomas nauju produktu su skaitmeniniais elementais, kuriam taikomas visas KAA. Tokiais atvejais pasikeičia bendras to produkto kibernetinio saugumo rizikos profilis, todėl pakeitimo negalima įvertinti neatsižvelgiant į visą produktą su skaitmeniniais elementais. Pakeitimą atliekančiam asmeniui viso pakeisto produkto su skaitmeniniais elementais atžvilgiu taikomos 13 ir 14 straipsniuose nustatytos gamintojo pareigos.

4.4.2. *Esminiai pakeitimai, kuriuos atlieka pirminis gamintojas*

122. Kai esminį pakeitimą atlieka pirminis gamintojas, įskaitant atvejus, kai programinės įrangos produktai su skaitmeniniais elementais kuriami iteraciniu būdu, tas gamintojas KAA taikymo tikslais ir toliau laikomas gamintoju, tačiau laikoma, kad iš esmės pakeistas produktas su skaitmeniniais elementais pateikiamas rinkai iš naujo.

123. Vadovaujantis Mėlynojo vadovo 2.1 skirsniu, pirminis gamintojas, pateikiantis rinkai iš esmės pakeistą produktą su skaitmeniniais elementais, gali pakartotinai naudoti esamus dokumentus ir bandymų rezultatus dėl tų produkto su skaitmeniniais elementais aspektų, kuriems esminis pakeitimas nedaro poveikio. Visų pirma, kai gamintojas rinkai pateikia iš esmės pakeistas to paties produkto su skaitmeniniais elementais versijas, atitikties vertinimo procedūra turėtų būti sutelkta į iš esmės pakeistas produkto su skaitmeniniais elementais dalis. Panašiai, kai atitikties vertinimą atlieka trečioji šalis, atitikties vertinimo įstaiga savo vertinimą turėtų sutelkti į iš esmės pakeistas dalis. Nepakeistų produkto su skaitmeniniais elementais dalių atžvilgiu ji gali pakartotinai naudoti esamus dokumentus ir bandymų rezultatus.

124. Pirmesniame poskirsnyje išdėstyti proporcingumo aspektai vienodai taikomi esminiams pakeitimams, kuriuos atlieka produkto su skaitmeniniais elementais, pateikto rinkai anksčiau nei 2027 m. gruodžio 11 d., pirminis gamintojas. Tai, kad pirminis gamintojas atlieka esminį pakeitimą, savaime nereiškia, kad gamintojas privalo užtikrinti visišką iki tos datos rinkai pateikto viso produkto su skaitmeniniais elementais atitiktį KAA, išskyrus atvejus, kai pakeitimas daro neigiamą poveikį viso produkto su skaitmeniniais elementais kibernetiniam saugumui. Kai pakeitimas viso produkto su skaitmeniniais elementais kibernetiniam saugumui poveikio nedaro, pirminio gamintojo pareigos, susijusios su tuo pakeitimu, turėtų būti taikomos tik iš esmės pakeistų dalių atžvilgiu.

5. **PALAIKYMO LAIKOTARPIS**

125. KAA 13 straipsnio 8 dalyje reikalaujama, kad gamintojai nustatytų palaikymo laikotarpį, kuriuo produkto su skaitmeniniais elementais, įskaitant jo komponentus, pažeidžiamumas būtų veiksmingai valdomas laikantis I priedo II dalyje nustatytų esminių reikalavimų. Palaikymo laikotarpis atspindi laikotarpį, kurį, kaip numatoma, produktas su skaitmeniniais elementais bus naudojamas, (tikėtiną naudojimo laiką) ir turėtų būti nustatomas atsižvelgiant į 13 straipsnio 8 dalyje nustatytus kriterijus, visų pirma į pagrįstus naudotojų lūkesčius, produkto su skaitmeniniais elementais pobūdį, įskaitant jo numatytąją paskirtį, taip pat į atitinkamus Sąjungos teisės aktus, kuriais nustatoma produktų su skaitmeniniais elementais naudojimo trukmė ([17]). Apskritai į šiuos kriterijus turi būti atsižvelgiama taip, kad nustatant palaikymo laikotarpį būtų užtikrintas proporcingumas.

([17]) Papildomi kriterijai, į kuriuos gali būti atsižvelgiama pagal 13 straipsnio 8 dalį, apima kitų gamintojų rinkai pateiktų panašias funkcijas atliekančių produktų su skaitmeniniais elementais palaikymo laikotarpius, veikimo aplinkos prieinamumą, integruotų komponentų, kurie atlieka pagrindines funkcijas ir yra gaunami iš trečiųjų šalių, palaikymo laikotarpius, taip pat atitinkamas KAA administracinio bendradarbiavimo grupės (ADCO) ir Komisijos pateiktas gaires.

126. 13 straipsnio 8 dalyje taip pat reikalaujama, kad palaikymo laikotarpis būtų ne trumpesnis kaip penkeri metai, išskyrus atvejus, kai numatoma, kad produktas su skaitmeniniais elementais bus naudojamas trumpiau nei penkerius metus, – tokiu atveju palaikymo laikotarpis turi atitikti numatomą naudojimo laiką. Taigi minimalus palaikymo laikotarpis yra tik apsaugos priemonė, kuria užtikrinama, kad pažeidžiamumas būtų valdomas pakankamai ilgą laiką, kartu suteikiant gamintojams galimybę atsižvelgti į produktus su skaitmeniniais elementais, kurių numatomas naudojimo laikas iš tiesų yra trumpesnis. 60 konstatuojamojoje dalyje šiuo klausimu pateikiama daugiau gairių ir paaiškinama, kad produktams su skaitmeniniais elementais, kuriuos pagrįstai numatoma naudoti ilgiau nei penkerius metus, atitinkamai turėtų būti nustatyti ilgesni palaikymo laikotarpiai. Todėl penkerių metų palaikymo laikotarpis neturėtų būti laikomas numatytuoju visiems produktams su skaitmeniniais elementais. Vietoj to gamintojas turėtų nustatyti tinkamą palaikymo laikotarpį atsižvelgdamas į 13 straipsnio 8 dalyje nurodytus kriterijus.

127. 13 straipsnio 19 dalyje reikalaujama, kad gamintojai pirkimo metu aiškiai ir suprantamai nurodytų palaikymo laikotarpio pabaigos datą (bent mėnesį ir metus). Joje taip pat reikalaujama, kad pasibaigus palaikymo laikotarpiui gamintojai pateiktų naudotojams atitinkamą pranešimą, kai tai techniškai įmanoma atsižvelgiant į produkto su skaitmeniniais elementais pobūdį. Šia pareiga siekiama užtikrinti naudotojams skaidrumą dėl laikotarpio, kuriuo jie gali tikėtis saugumo palaikymo, trukmės.

128. Programinės įrangos produktų su skaitmeniniais elementais, kurie dažnai kuriami ir išleidžiami iteraciniu būdu ir kurių iš esmės pakeistos versijos ilgainiui gali būti dažnai pateikiamos rinkai, palaikymo laikotarpis turi būti suprantamas atsižvelgiant į tokį kūrimo modelį. Pateikiant rinkai kiekvieną iš esmės pakeistą programinės įrangos produkto su skaitmeniniais elementais versiją turi būti deklaruojamas 13 straipsnio 8 dalies reikalavimus atitinkantis palaikymo laikotarpis. Tai apima minimalų ne trumpesnį kaip penkerių metų palaikymo laikotarpį, išskyrus atvejus, kai galima įrodyti, kad numatomas tos versijos naudojimo laikas yra trumpesnis, kaip paaiškinta ir 60 konstatuojamojoje dalyje. *5.1* skirsnyje „*Esminiai pakeitimai ir palaikymo laikotarpis*“ papildomai paaiškinama, kad tais atvejais, kai dėl esminio pakeitimo nesikeičia veiksniai, kuriais remiantis iš pradžių buvo nustatytas numatomas produkto su skaitmeniniais elementais naudojimo laikas, pradinis palaikymo laikotarpis lieka nepakitęs (įskaitant atvejus, kai likęs palaikymo laikotarpis yra trumpesnis nei penkeri metai).

129. 13 straipsnio 10 dalyje programinės įrangos produktų su skaitmeniniais elementais atžvilgiu numatytas lankstumas: gamintojams leidžiama tam tikromis sąlygomis užtikrinti atitiktį I priedo II dalies 2 punkte nustatytam pažeidžiamumo valdymo (pažeidžiamumo šalinimo ir ištaisymo) reikalavimui tik tos programinės įrangos produkto su skaitmeniniais elementais versijos, kuri rinkai buvo pateikta vėliausiai, atžvilgiu. Tai leidžiama, kai anksčiau pateiktų versijų naudotojai gali nemokamai gauti vėliausiai rinkai pateiktą versiją ir nepatiria papildomų išlaidų, susijusių su aparatinės ir programinės įrangos aplinkos, kurioje jie naudoja pirminę to produkto versiją, pritaikymu.

130. 13 straipsnio 10 dalies taikymo tikslais sąvoka „papildomos išlaidos“ turėtų būti aiškinama praktiškai ir proporcingai, atsižvelgiant į įprastą ir numatomą programinės įrangos priežiūros ir eksploatavimo praktiką. Ji neapima pagrįstų veiklos pastangų, kurios yra neatsiejamos nuo programinės įrangos naujinių diegimo arba saugios veikimo aplinkos palaikymo, pavyzdžiui, darbuotojų darbo laiko, įprastinių bandymų, konfigūracijos pakeitimų ar bazinių programinės įrangos priklausomybės santykių atnaujinimo, kai tai būtina dėl komponentų gyvavimo ciklo pabaigos arba žinomų saugumo pažeidžiamumų. Priešingai, sąvoka „papildomos išlaidos“ reiškia naštą, viršijančią tai, ko paprastai galima tikėtis programinės įrangos naujinimo atveju, pavyzdžiui, privalomą naujos aparatinės įrangos įsigijimą, infrastruktūros pakeitimą arba esminius veikimo aplinkos pakeitimus.

131. Nuolat tobulinamų programinės įrangos produktų su skaitmeniniais elementais gamintojai per palyginti trumpus laikotarpius gali rinkai vieną po kitos pateikti iš esmės pakeistas versijas ir tikėtis, kad naudotojai reguliariai pereis prie naujesnių versijų. Tokiais atvejais kiekvienos iš esmės pakeistos versijos deklaruotasis palaikymo laikotarpis turi atitikti 13 straipsnio 8 dalies reikalavimus tuo metu, kai ji pateikiama rinkai. Kitaip tariant, gamintojas turi deklaruoti naują tos iš esmės pakeistos versijos palaikymo laikotarpį. Tačiau gamintojai gali remtis 13 straipsnio 10 dalimi ir nustoti šalinti bei taisyti ankstesnių versijų pažeidžiamumą, kai naudotojai gali nemokamai ir

nepatirdami pirmiau nurodytų papildomų išlaidų pereiti prie naujesnės versijos, net jeigu dėl to faktinis tų ankstesnių versijų palaikymo laikotarpis tampa trumpesnis ([18]). Gamintojui ir toliau taikomi kiti I priedo II dalyje nustatyti pažeidžiamumo valdymo reikalavimai, taip pat 14 straipsnyje nustatytos pareigos pranešti. Kaip paaiškinta ir 40 konstatuojamojoje dalyje, tie reikalavimai, be kita ko, apima šiuos visoms vėliau rinkai pateikiamų iš esmės pakeistų programinės įrangos produkto su skaitmeniniais elementais versijų atžvilgiu taikomus reikalavimus: i) laikytis pažeidžiamumo koordinuoto atskleidimo politikos ir ii) taikyti priemones, kuriomis palengvinamas dalijimasis informacija apie galimą pažeidžiamumą ([19]).

52 pavyzdys. Gamintojas pateikia ES rinkai išmaniojo telefono modelį ir deklaruoja X metų palaikymo laikotarpį nuo pateikimo rinkai dienos, per kurį jis teiks saugumo naujinius, skirtus pažeidžiamumui šalinti. Per šį laikotarpį gamintojas reguliariai išleidžia programinės įrangos naujinius ir iš esmės pakeistas operacinės sistemos versijas, kurias naudotojai gali nemokamai įdiegti ir tam nereikia naujos aparatinės įrangos.

Pagal 13 straipsnio 10 dalį gamintojas gali nuspręsti šalinti ir taisyti pažeidžiamumą tik naujausioje tam išmaniojo telefono modeliui teikiamoje operacinės sistemos versijoje, jeigu ankstesnes versijas galima nemokamai pakeisti naujausia versija ir dėl to nepatiriama papildomų išlaidų. Visą palaikymo laikotarpį gamintojui ir toliau taikomi kiti pažeidžiamumo valdymo reikalavimai, pavyzdžiui, koordinuoto pažeidžiamumo atskleidimo ir dalijimosi informacija priemonės.

53 pavyzdys. Gamintojas pateikia rinkai įmonėms skirtą programinės įrangos produktą su skaitmeniniais elementais ir kas kelis mėnesius išleidžia iš esmės pakeistas jo versijas, kuriose įdiegti saugumo patobulinimai, naujos funkcijos ir užtikrintas suderinamumas su atnaujintomis operacinėmis sistemomis bei platformomis. Kiekvieną versiją pateikiant rinkai turi būti pagal 13 straipsnio 8 dalį deklaruojamas palaikymo laikotarpis. Gamintojas tikisi, kad naudotojai, įprastai eksploatuodami produktą, reguliariai pereis prie naujesnių versijų, ir suteikia galimybę nemokamai gauti naujausią versiją. Naujiniams diegti gali reikėti pagrįstų veiklos pastangų, pavyzdžiui, bandymų ar konfigūracijos pakeitimų, tačiau dėl to nepatiriama papildomų išlaidų, pavyzdžiui, nereikia įsigyti naujos aparatinės įrangos ar iš esmės keisti infrastruktūros. Tokiomis aplinkybėmis gamintojas gali remtis 13 straipsnio 10 dalimi ir nustoti šalinti bei taisyti ankstesnių versijų pažeidžiamumą, kai naudotojai gali pereiti prie naujausios versijos, kartu ir toliau laikydamasis kitų pažeidžiamumo valdymo reikalavimų visų vėliau išleidžiamų iš esmės pakeistų versijų atžvilgiu.

5.1. **Esminiai pakeitimai ir palaikymo laikotarpis**

132. Kaip nustatyta 4.4 skirsnyje „*Esminio pakeitimo pasekmės*“, kai produkto su skaitmeniniais elementais pakeitimas laikomas esminiu pakeitimu ir pakeistas produktas su skaitmeniniais elementais tiekiamas rinkai, KAA taikymo tikslais jis turi būti laikomas nauju produktu, o iš esmės pakeisto produkto su skaitmeniniais elementais tiekimas rinkai laikomas nauju pateikimu rinkai. Todėl tikslinga paaiškinti, kokį poveikį šis naujas pateikimas rinkai turi iš esmės pakeisto produkto su skaitmeniniais elementais palaikymo laikotarpiui.

133. Iš esmės pakeisto produkto su skaitmeniniais elementais palaikymo laikotarpis turėtų būti nustatomas atsižvelgiant į numatomą to produkto naudojimo laiką ir KAA 13 straipsnio 8 dalyje nustatytus kriterijus. Taigi dėl esminio pakeitimo turėtų būti atliktas naujas vertinimas pagal šiuos kriterijus, tačiau tai savaime nereiškia, kad palaikymo laikotarpis turi būti pradėtas skaičiuoti iš naujo ar net pratęstas. Aktualus klausimas yra tai, ar esminis pakeitimas daro poveikį veiksniams, kuriais remiantis iš pradžių buvo nustatytas numatomas to produkto naudojimo laikas, taigi ir pradinis palaikymo laikotarpis.

([18]) Primintina, jog 13 straipsnio 19 dalyje reikalaujama, kad gamintojai, kai tai techniškai įmanoma atsižvelgiant į produkto su skaitmeniniais elementais pobūdį, pateiktų naudotojams pranešimą, kuriuo jie informuojami, kad jų produkto su skaitmeniniais elementais palaikymo laikotarpis baigėsi. Todėl, kai nustojama šalinti ir taisyti ankstesnių versijų pažeidžiamumą, tikimasi, kad naudotojai, kurie neperėjo prie naujausios versijos, apie tai bus informuoti, jeigu tai techniškai įmanoma.

([19]) Pažymėtina, kad tais atvejais, kai naudotojai gali pereiti prie naujausios programinės įrangos versijos nepatirdami papildomų išlaidų, gamintojai vis dėlto gali pasirinkti ir toliau šalinti bei taisyti ankstesnių tos programinės įrangos versijų pažeidžiamumą, be kita ko, už atlygį arba pagal kitus komercinius susitarimus. KAA nereikalaujama, kad gamintojai tokių ankstesnių versijų saugumo naujinius teiktų nemokamai.

134. Kai esminis pakeitimas poveikio tiems veiksniams nedaro, numatomas naudojimo laikas, remiantis 13 straipsnio 8 dalyje nustatytais kriterijais, lieka toks pats, koks buvo nustatytas iš pradžių, todėl pakeisto produkto su skaitmeniniais elementais palaikymo laikotarpis turėtų atitikti likusį numatomą pirminio rinkai pateikto produkto naudojimo laiką. Paprastai taip būna tais atvejais, kai numatomas naudojimo laikas yra nustatytas visų pirma remiantis veiksniais, kurių pakeitimas nekeičia, pavyzdžiui, aparatinės įrangos komponentų fiziniu patvarumu, o esminis pakeitimas susijęs tik su programinės įrangos funkcionalumu arba galinėmis paslaugomis.

54 pavyzdys. Gamintojas pateikia rinkai dulkių siurblį robotą, kurio numatomas naudojimo laikas, nustatytas atsižvelgiant į produkto su skaitmeniniais elementais pobūdį, įskaitant aparatinės įrangos komponentų fizinį patvarumą ir nusidėvėjimo charakteristikas, taip pat į pagrįstus naudotojų lūkesčius dėl šio produkto naudojimo trukmės, yra X metų. Gamintojas nustato X metų palaikymo laikotarpį. Po Y metų gamintojas išleidžia programinės įrangos naujinį, kuris laikomas esminiu pakeitimu ir kuriuo įdiegiami nauji valymo režimai bei navigacijos funkcijos. Programinės įrangos naujinys nedaro poveikio aparatinės įrangos fiziniam patvarumui ir nekeičia pagrįstų naudotojų lūkesčių dėl šio produkto naudojimo trukmės. Todėl, remiantis 13 straipsnio 8 dalyje nustatytais kriterijais, numatomas naudojimo laikas lieka toks pats. Pakeisto produkto su skaitmeniniais elementais palaikymo laikotarpis atitinka likusį iš pradžių nustatytą numatomą naudojimo laiką.

55 pavyzdys. Gamintojas pateikia rinkai sudėtingą pramoninių mašinų gaminį su skaitmeniniais elementais, su debesijos galine sistema, kuri yra nuotolinio duomenų tvarkymo sprendinys. Numatomas naudojimo laikas, nustatytas atsižvelgiant į pagrįstus naudotojų lūkesčius ir produkto su skaitmeniniais elementais pobūdį, kaip antai mašinos aparatinės įrangos fizinį patvarumą ir numatomą nusidėvėjimą, yra X metų. Palaikymo laikotarpis nustatomas taip, kad atitiktų šį numatomą X metų naudojimo laiką. Po Y metų gamintojas pertvarko debesijos galinės sistemos (nuotolinio duomenų apdorojimo sprendinio) architektūrą, įdiegdamas naujas API ir duomenų srautus, ir šis pakeitimas laikomas esminiu produkto su skaitmeniniais elementais pakeitimu, tačiau nekeičia produkto pobūdžio ir nedaro poveikio naudotojų lūkesčiams. Todėl, remiantis 13 straipsnio 8 dalyje nustatytais kriterijais, numatomas naudojimo laikas lieka toks pats. Pakeisto produkto su skaitmeniniais elementais palaikymo laikotarpis atitinka likusį iš pradžių nustatytą numatomą naudojimo laiką.

135. Kai esminis pakeitimas daro poveikį veiksniams, kuriais remiantis iš pradžių buvo nustatytas numatomas produkto su skaitmeniniais elementais naudojimo laikas, gamintojas turėtų iš naujo apskaičiuoti palaikymo laikotarpį, kad jis atitiktų naują numatomą naudojimo laiką, atitinkamai taikydamas 13 straipsnio 8 dalyje nustatytus kriterijus. Taip gali būti, pavyzdžiui, tais atvejais, kai atliekami aparatinės įrangos atnaujinimo pakeitimai, kuriais pratęsiama produkto eksploatavimo trukmė, arba kai iš esmės perprogramuojama ar perrašoma pagrindinė produkto programinė įranga ir dėl to reikšmingai pasikeičia numatomas jo naudojimo laikas ([20]).

56 pavyzdys. Gamintojas pateikia rinkai programuojamąjį loginį valdiklį (PLC), kurio numatomas naudojimo laikas, nustatytas visų pirma atsižvelgiant į produkto su skaitmeniniais elementais pobūdį ir jame naudojamos aparatinės įrangos patvarumą, yra X metų. Nustatomas atitinkamas palaikymo laikotarpis. Praėjus keleriems metams nuo pirminio pateikimo rinkai, gamintojas atlieka esminį pakeitimą – pakeičia PLC integruotąją kompiuterinę platformą, įskaitant procesorių, atmintinę ir vykdymo aplinką, naujos kartos komponentais, suprojektuotais kur kas ilgesnei eksploatavimo trukmei. Dėl šio pakeitimo keičiasi pagrįsti naudotojų lūkesčiai ir produkto su skaitmeniniais elementais pobūdis: PLC naudotojas dabar gali pagrįstai tikėtis, kad, naudojant naująją kompiuterinę platformą, PLC produktyvaus naudojimo laikas bus ilgesnis už iš pradžių deklaruotą numatomą jo naudojimo laiką. Todėl, remiantis 13 straipsnio 8 dalyje nustatytais kriterijais, numatomas naudojimo laikas yra ilgesnis ir gamintojas atitinkamai iš naujo apskaičiuoja konkretaus PLC palaikymo laikotarpį.

6. **SVARBŪS IR YPATINGOS SVARBOS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS**

136. KAA 7 straipsnio 1 dalyje nustatyta, kad produktai su skaitmeniniais elementais, turintys pagrindinę reglamento III priede nustatytos produktų kategorijos funkciją, laikomi „svarbiais produktais su skaitmeniniais elementais“. III priede svarbūs produktai su skaitmeniniais elementais toliau skirstomi į I ir II klases. Panašiai 8 straipsnio 1 dalyje nustatyta, kad produktai su skaitmeniniais elementais, turintys pagrindinę KAA IV priede nustatytos produktų kategorijos funkciją, laikomi „ypatingos svarbos produktais su skaitmeniniais elementais“ ([21]).

([20]) Primintina, kad, kaip nurodyta 4.1 skirsnyje „*Fizinis taisymas*“, atnaujinimo, techninės priežiūros ar taisymo darbai paprastai nelaikomi esminiais pakeitimais.

([21]) Komisijos įgyvendinimo reglamente (ES) 2025/2392 pateikiamas svarbių ir ypatingos svarbos produktų kategorijų techninis aprašas.

137. Produkto su skaitmeniniais elementais priskyrimas svarbių ar ypatingos svarbos produktų kategorijai arba, priešingai, įprastinių produktų kategorijai ([22]) yra svarbus nustatant atitikties vertinimo procedūrą, kurią pagal 32 straipsnį gamintojas turi atlikti prieš pateikdamas tą produktą su skaitmeniniais elementais rinkai. Pažymėtina, kad įprastinių produktų kategorijai priskirtiems produktams su skaitmeniniais elementais visada gali būti taikoma A moduliu grindžiama vidaus kontrolės procedūra (įsivertinimas) ([23]). I arba II klasės svarbiems produktams su skaitmeniniais elementais ir ypatingos svarbos produktams su skaitmeniniais elementais taikomos griežtesnės atitikties vertinimo procedūros. Tai netaikoma I arba II klasės svarbiems produktams su skaitmeniniais elementais, kurie yra laisvoji ir atviroji programinė įranga ir yra pateikiami rinkai – pagal 32 straipsnio 5 dalį tokių produktų gamintojams leidžiama taikyti įprastinių produktų kategorijai nustatytas procedūras.

138. Todėl savoka „pagrindinė funkcija“ (angl. *core functionality*) yra esminė gamintojui nustatant, kokia atitikties vertinimo tvarka yra taikytina. Tačiau ši sąvoka KAA nėra aiškiai apibrėžta. Produktai su skaitmeniniais elementais gali atlikti įvairias funkcijas, iš kurių kai kurios gali būti pagalbinės jų pagrindinės funkcijos atžvilgiu ir neturėtų daryti įtakos produkto priskyrimui įprastinių produktų kategorijai, I ar II klasės svarbių produktų kategorijai arba ypatingos svarbos produktų kategorijai. Todėl tikslinga pateikti išsamesnes gaires, kurios gamintojams padėtų tinkamai atlikti atitinkamas atitikties vertinimo procedūras, o rinkos priežiūros institucijoms – užtikrinti suderintą KAA vykdymą visoje ES.

6.1. **Pagrindinė funkcija**

139. Produkto su skaitmeniniais elementais pagrindinė funkcija – tai pagrindinės to produkto savybės ir techninės galimybės, be kurių jis negalėtų atlikti numatytosios paskirties. Ji gali būti vertinama atsižvelgiant į konkrečias to produkto naudojimo aplinkybes ir sąlygas, be kita ko, į informaciją, kurią gamintojas pateikia naudojimo instrukcijose, reklaminėje ar pardavimo medžiagoje ir pareiškimuose, taip pat techniniuose dokumentuose.

57 pavyzdys. Programinės įrangos produktas su skaitmeniniais elementais sudaro abstrakcijos lygmenį virš bazinės aparatinės įrangos lygmens ir valdo programinės įrangos komponentų vykdymą. Pagrindinės jo savybės apima aparatinės įrangos ir išorinių įrenginių inicijavimą, procesų ir atminties valdymą, įvesties ir išvesties valdymą, užduočių planavimą, išteklių paskirstymą, taip pat sistemos paslaugų ir taikomųjų programų sąsajų (API), per kurias taikomosios programos sąveikauja su įrenginio aparatinės ir programinės įrangos ištekliais, teikimą. Techniniuose dokumentuose nurodoma, kad produktas su skaitmeniniais elementais koordinuoja kompiuterijos išteklius, užtikrina sistemos konfigūracijų laikymąsi ir suteikia standartizuotas sąsajas programinės įrangos moduliams bei prijungtiems išoriniams įrenginiams. Gamintojas pabrėžia, kad šie pajėgumai leidžia platformai veikti kaip centrinei programinės įrangos aplinkai, kurioje gali patikimai veikti taikomosios programos. Produkto su skaitmeniniais elementais pagrindinė funkcija yra operacinės sistemos, apibūdintos Įgyvendinimo reglamento (ES) 2025/2392 I priedo 11 punkte, funkcija.

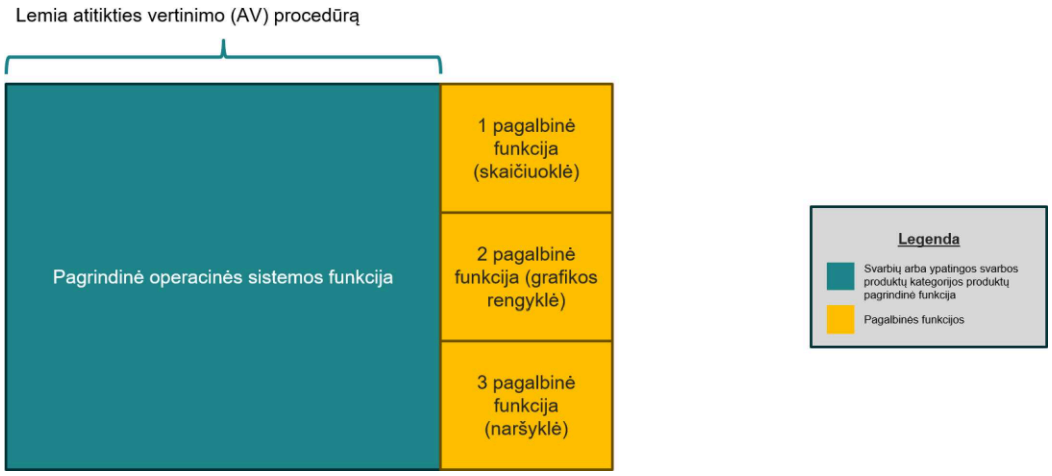
140. Produkto su skaitmeniniais elementais funkcionalumas retai apsiriboja vien jo pagrindine funkcija, nes produktai su skaitmeniniais elementais dažnai (jei ne visada) atlieka papildomas funkcijas, kurios neprisideda prie produkto pagrindinės funkcijos. Tai taip pat gali apimti komponentų, kurie patys atlieka kitam svarbiam ar ypatingos svarbos produktui su skaitmeniniais elementais būdingas funkcijas, integravimą. Tačiau vien tai, kad produktas su skaitmeniniais elementais atlieka kitokias funkcijas nei tos, kurios nurodytos svarbių ar ypatingos svarbos produktų su skaitmeniniais elementais techniniuose aprašuose, arba jas papildo, savaime neužkerta kelio laikyti tokį produktą atliekančiu vieną iš tokių pagrindinių funkcijų.

([22]) Įprastinių (angl. *default*) produktų kategorija KAA nėra apibrėžta. Šiame dokumente ši sąvoka vartojama produktams su skaitmeniniais elementais, kurių pagrindinė funkcija neatitinka nė vienos iš KAA III arba IV priede nurodytų kategorijų produktų funkcijų ir kuriems dėl to taikoma 32 straipsnio 1 dalyje nustatyta atitikties vertinimo tvarka, apibūdinti.

([23]) Vis dėlto gamintojas visada gali pasirinkti taikyti griežtesnę atitikties vertinimo procedūrą, kaip nustatyta 32 straipsnio 1 dalyje.

2 pav

Iliustracija, kaip pagrindinė funkcija, o ne pagalbinės funkcijos, lemia taikytiną atitikties vertinimo procedūrą



141. Produktas su skaitmeniniais elementais gali gebėti atlikti svarbių ar ypatingos svarbos produktų kategorijos produktams būdingas funkcijas, tačiau jo pagrindinė funkcija vis vien gali skirtis nuo tokios kategorijos produktų pagrindinės funkcijos. Tokiais atvejais toks produktas su skaitmeniniais elementais nebūtų laikomas svarbiu ar ypatingos svarbos produktu su skaitmeniniais elementais. Kaip aiškiai nustatyta KAA 7 straipsnio 1 dalyje dėl svarbių produktų su skaitmeniniais elementais (ir taikant tą pačią logiką ypatingos svarbos produktams su skaitmeniniais elementais), vien svarbaus ar ypatingos svarbos produkto su skaitmeniniais elementais integravimas savaime nereiškia, kad produktas su skaitmeniniais elementais tampa svarbiu ar ypatingos svarbos produktu su skaitmeniniais elementais.

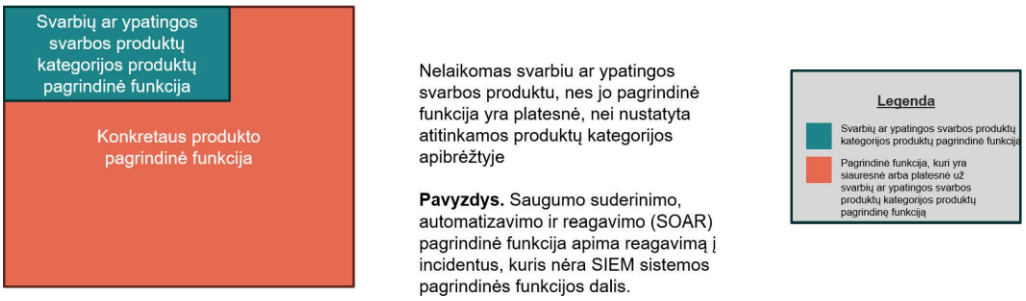
58 pavyzdys. Išmaniajame telefone integruojama operacinė sistema, atliekanti Įgyvendinimo reglamento (ES) 2025/2392 I priedo 11 punkte apibūdintas funkcijas. Nors ši operacinė sistema leidžia valdyti aparatinės įrangos išteklius ir vykdyti taikomosios programinės įrangos programas, viso išmaniojo telefono pagrindinė funkcija yra kita (pvz., suteikti naudotojams galimybę bendrauti ir gauti informaciją bei paslaugas). Vien operacinės sistemos integravimas nereiškia, kad išmanusis telefonas turi operacinei sistemai būdingą pagrindinę funkciją.

142. Kai kurie produktai su skaitmeniniais elementais gali būti panašūs į svarbių ar ypatingos svarbos produktų kategorijos produktus arba priklausyti tai pačiai bendrajai produktų grupei, tačiau jų pagrindinė funkcija gali būti kur kas platesnė arba kur kas siauresnė už tos kategorijos produktų pagrindinę funkciją. Taip nėra tuo atveju, kai produktas su skaitmeniniais elementais turi papildomų funkcijų, kurios tik papildo arba išplečia pagrindinę funkciją, o ši pati atitinka svarbių ar ypatingos svarbos produktų kategorijos produktų pagrindinę funkciją; tokiais atvejais produktas su skaitmeniniais elementais išlaiko tos kategorijos produktų pagrindinę funkciją ir yra atitinkamai klasifikuojamas. Šis vertinimas turėtų būti grindžiamas pagrindinėmis produkto savybėmis ir techninėmis galimybėmis, objektyviai įvertintomis atsižvelgiant į jo numatytąją paskirtį, o ne tuo, kaip produktas su skaitmeniniais elementais apibūdinamas ar reklamuojamas, jei toks apibūdinimas neatspindi faktinių produkto techninių charakteristikų.

59 pavyzdys. Saugumo suderinimo, automatizavimo ir reagavimo (SOAR) programinė įranga dažnai gali atlikti produktų su skaitmeniniais elementais, priklausančių „saugumo informacijos ir įvykių valdymo (SIEM) sistemų“ kategorijai, funkcijas, t. y. rinkti duomenis iš įvairių šaltinių, juos analizuoti bei susieti ir pateikti kaip informaciją, kuria remiantis galima imtis su saugumu susijusių veiksmų. Tačiau tokios programinės įrangos pagrindinė funkcija yra kur kas platesnė nei SIEM sistemų, nes jos techninių galimybių pagrindiniai elementai apima, be kita ko, reagavimo į incidentus paslaugas. Todėl paprastai nelaikoma, kad SOAR programinė įranga turi SIEM sistemų pagrindinę funkciją.

3 pav

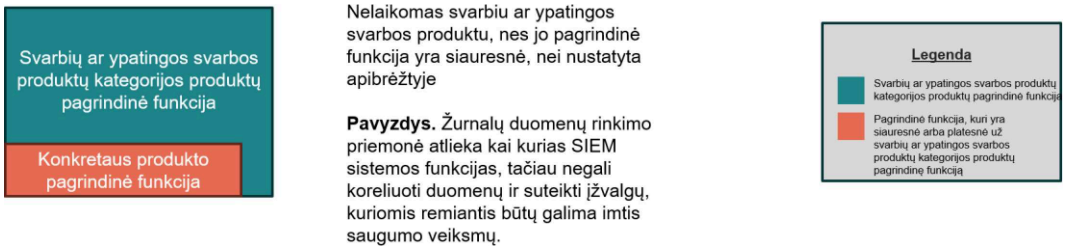
Atvejo, kai produkto su skaitmeniniais elementais pagrindinė funkcija yra kur kas platesnė, nei nustatyta svarbių ar ypatingos svarbos produktų kategorijos apibrėžtyje, iliustracija



60 pavyzdys. Tam tikros žurnalų duomenų rinkimo ir vizualizavimo priemonės gali priimti žurnalų duomenis ir pateikti pagrindines suvestines, kuriose rodomi sistemos įvykiai. Nors tokios priemonės gali būti naudojamos saugumo stebėsenos veiklai, jų pagrindinė funkcija yra kur kas siauresnė nei SIEM sistemų, nes jos neatlieka duomenų koreliavimo ir nesuteikia įžvalgų, kuriomis remiantis būtų galima imtis saugumo veiksmų. Todėl paprastai nelaikoma, kad tokios priemonės turi SIEM sistemų pagrindinę funkciją.

4 pav

Atvejo, kai produkto su skaitmeniniais elementais pagrindinė funkcija yra kur kas siauresnė, nei nustatyta svarbių ar ypatingos svarbos produktų kategorijos apibrėžtyje, iliustracija

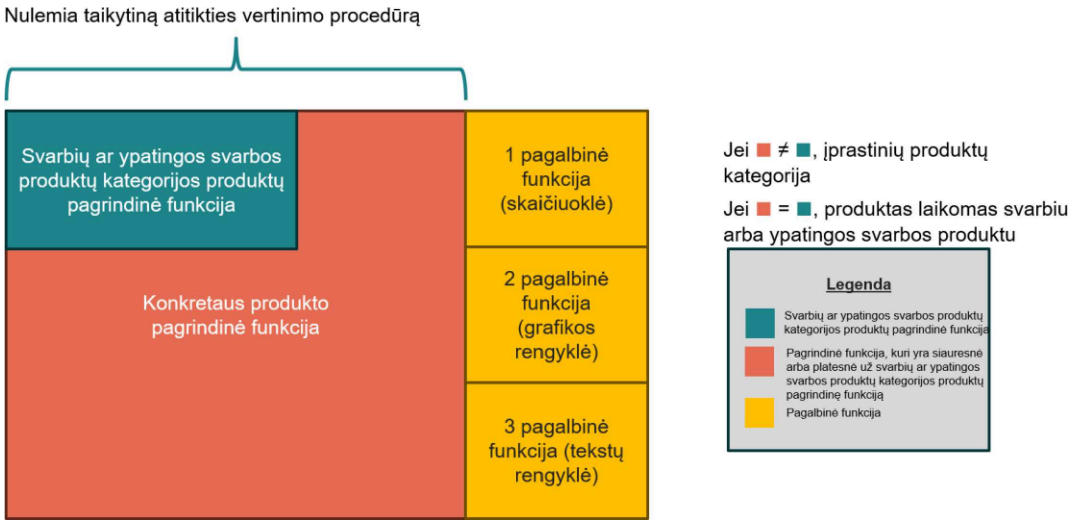


143. Gamintojas negali klaidinamai pristatyti savo produkto su skaitmeniniais elementais pagrindinės funkcijos, kad išvengtų svarbiems ar ypatingos svarbos produktams su skaitmeniniais elementais taikomos atitikties vertinimo tvarkos, pavyzdžiui, pernelyg sureikšmindamas arba sumenkindamas tam tikrų funkcijų vaidmenį, kad atrodytų, jog produkto funkcijos kur kas platesnės arba kur kas siauresnės už tam tikrą pagrindinę funkciją. Taip būtų, pavyzdžiui, tais atvejais, kai reklaminė medžiaga, naudojimo instrukcijos ir techniniai dokumentai akivaizdžiai prieštarauja vieni kitiems.

144. Nustatant taikytiną atitikties vertinimo tvarką negali būti laikoma, kad produktas su skaitmeniniais elementais turi daugiau kaip vieną pagrindinę funkciją. Pagal KAA VII priedą gamintojai produkto techniniuose dokumentuose privalo aprašyti savo produkto su skaitmeniniais elementais numatytąją paskirtį ir nurodyti taikytą atitikties vertinimo procedūrą. Todėl produkto pagrindinė funkcija turėtų būti aiškiai nustatyta. Tai leidžia teisingai nustatyti taikytiną atitikties vertinimo tvarką ir sudaro sąlygas rinkos priežiūros institucijoms prižiūrėti ir tikrinti, ar reglamentas taikomas tinkamai.

5 pav

Iliustracija, kaip konkretaus produkto su skaitmeniniais elementais pagrindinė funkcija lemia produkto klasę, taigi ir taikytiną atitikties vertinimo procedūrą



145. Kai kurie produktai su skaitmeniniais elementais pateikiami rinkai kaip pavieniai produktai su skaitmeniniais elementais, tačiau juos sudaro atskiri moduliai, atliekantys skirtingas funkcijas. Jeigu gamintojas tuos modulius taip pat atskirai tiekia rinkai, pavyzdžiui, kai jie siūlomi atskirai įsigyti, licencijuoti ar prenumeruoti, kiekvienas toks modulis pats yra savarankiškas produktas su skaitmeniniais elementais. Todėl tokie moduliai klasifikuojami pagal kiekvieno iš jų pagrindinę funkciją (taigi pagal kiekvieno modulio pagrindinę funkciją taikoma atitinkama atitikties vertinimo tvarka). Tai nedaro poveikio moduliams, kurie tiekiami tik kaip integruoto produkto su skaitmeniniais elementais komponentai ir rinkai atskirai netiekiami; tokiais atvejais pagrindinė funkcija nustatoma viso integruoto produkto su skaitmeniniais elementais lygmeniu.

61 pavyzdys. Gamintojas pateikia rinkai integruotą saugumo priemonių rinkinį, kurį sudaro keli moduliai, įskaitant SIEM sistemą, įsibrovimo aptikimo sistemą ir analizės modulį. Gamintojas šiuos modulius taip pat siūlo prenumeruoti atskirai. Pagal šį scenarijų kiekvienas modulis yra atskiras produktas su skaitmeniniais elementais ir klasifikuojamas pagal jo pagrindinę funkciją. SIEM moduliui taikoma I klasės svarbiems produktams su skaitmeniniais elementais nustatyta atitikties vertinimo tvarka, nes jo pagrindinė funkcija atitinka „saugumo informacijos ir įvykių valdymo (SIEM) sistemų“ pagrindinę funkciją. Įsibrovimo aptikimo sistemai taikoma II klasės svarbiems produktams su skaitmeniniais elementais nustatyta atitikties vertinimo tvarka, nes jos pagrindinė funkcija atitinka „užkardų, įsibrovimo aptikimo ir prevencijos sistemų“ pagrindinę funkciją. Analizės moduliui taikoma įprastinių produktų kategorijos produktams su skaitmeniniais elementais nustatyta atitikties vertinimo tvarka, nes jo pagrindinė funkcija neatitinka nė vienos svarbių ar ypatingos svarbos produktų kategorijos pagrindinės funkcijos.

146. Už KAA 32 straipsnyje nustatytų pareigų nevykdymą gali būti pagal 64 straipsnio 3 dalį skiriamos administracinės baudos.

6.2. Svarbių ir ypatingos svarbos produktų su skaitmeniniais elementais atitikties vertinimas

147. Nustatęs savo produkto su skaitmeniniais elementais pagrindinę funkciją, gamintojas turi atlikti vieną iš taikytinų atitikties vertinimo procedūrų. Gamintojas turi užtikrinti, kad visas produktas su skaitmeniniais elementais atitiktų esminius reikalavimus, atitinkamai atsižvelgdamas į jame integruotų komponentų ar funkcijų saugumą.

148. Griežtesnė atitikties vertinimo procedūra, kurioje dalyvauja trečioji šalis (remiantis B ir C moduliais, H moduliu arba kibernetinio saugumo sertifikavimo schemomis), yra privaloma II klasės svarbiems produktams su skaitmeniniais elementais (išskyrus produktus, kurie pagal 32 straipsnio 5 dalį laikomi laisvąja ir atvirąja programine įranga) ir ypatingos svarbos produktams su skaitmeniniais elementais ([24]). Tačiau I klasės svarbiems produktams su skaitmeniniais elementais (išskyrus produktus, kurie pagal 32 straipsnio 5 dalį laikomi laisvąja ir atvirąja programine įranga) trečiosios šalies atliekama atitikties vertinimo procedūra yra privaloma tik tuo atveju, jei gamintojas netaikė arba tik iš dalies taikė atitinkamus darniuosius standartus, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, (toliau – darnieji standartai), bendrąsias specifikacijas arba Europos kibernetinio saugumo sertifikavimo schemas, kurių saugumo užtikrinimo lygis yra bent „pakankamai aukštas“ ([25]).

149. Todėl tam, kad I klasės svarbiam produktui su skaitmeniniais elementais būtų galima taikyti vidaus kontrolės procedūrą, i) turi būti taikomi visi taikytini atitinkamo darniojo standarto reikalavimai ir ii) standarto taikymo sritis turi apimti bent visą kibernetinio saugumo riziką, susijusią su to produkto pagrindine funkcija.

150. Produkto su skaitmeniniais elementais aprėptis gali būti platesnė nei numatytoji atitinkamame darniajame standarte, o tokios papildomos funkcijos gali kelti kitokią arba papildomą kibernetinio saugumo riziką. Gamintojas visais atvejais privalo atlikti rizikos vertinimą pagal 13 straipsnio 2 dalį, todėl turėtų patikrinti, ar įgyvendinant darnųjį standartą apimama visa su produktu su skaitmeniniais elementais susijusi rizika. Jei įgyvendinant standartą apimama ne visa rizika, gamintojas turėtų kitomis priemonėmis užtikrinti, kad jo produktas su skaitmeniniais elementais atitiktų esminius reikalavimus.

151. Todėl, jei I klasės svarbaus produkto su skaitmeniniais elementais gamintojas taikė atitinkamą darnųjį standartą, apimantį su to produkto pagrindine funkcija susijusią riziką, jis gali nuspręsti savo produkto atitikčiai reikalavimams įrodyti taikyti vidaus kontrolės procedūrą. Vykdydamas atitikties vertinimo veiklą gamintojas vis vien privalės įrodyti, kad visa su jo produktu su skaitmeniniais elementais susijusi rizika yra valdoma. Todėl, jei darniojo standarto taikymo sritis neapima viso produkto su skaitmeniniais elementais, gamintojas vis vien turi dokumentuose nurodyti, kokias papildomas priemones jis įgyvendino šiai rizikai valdyti.

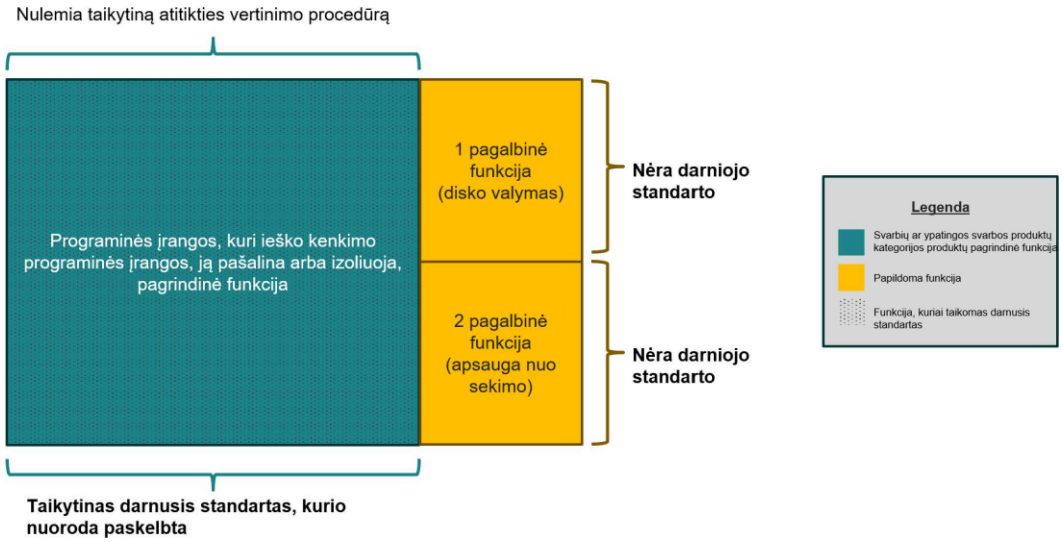
62 pavyzdys. Antivirusinės programinės įrangos pagrindinė funkcija yra ieškoti kenkimo programinės įrangos, ją pašalinti arba izoliuoti, kaip nurodyta Įgyvendinimo reglamento (ES) 2025/2392 I priedo 4 punkte. Šis produktas su skaitmeniniais elementais taip pat turi papildomų funkcijų, būtent disko valymo funkciją ir apsaugos nuo sekimo funkciją, kuri apsaugo naudotoją, kai jis naršo internete. Gamintojas atlieka viso produkto su skaitmeniniais elementais rizikos vertinimą, apimantį antivirusinės programos pagrindinę funkciją, disko valymo ir apsaugos nuo sekimo funkcijas. Jis taiko darnųjį standartą, apimantį su antivirusinės programinės įrangos pagrindine funkcija susijusią riziką, ir papildomas priemones, skirtas papildomų funkcijų keliamai rizikai valdyti. Gamintojas gali naudoti vidaus kontrolės procedūrą savo atitikties vertinimui, apimančiam visą produktą su skaitmeniniais elementais, įskaitant disko valymo ir apsaugos nuo sekimo funkcijas.

([24]) Taip yra ir tuo atveju, kai naudojama Europos kibernetinio saugumo sertifikavimo schema, kurios saugumo užtikrinimo lygis yra bent „pakankamai aukštas“, nes pagal tokią schemą yra privalomas trečiosios šalies – sertifikavimo įstaigos – dalyvavimas.

([25]) Siekiant glaustumo, likusioje šio skirsnio dalyje nurodomi tik darnieji standartai, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*. Tačiau tos pačios gairės taip pat taikomos pagal 27 straipsnio 2 dalį priimtoms bendrosioms specifikacijoms ir Europos kibernetinio saugumo sertifikavimo schemoms, kai Komisija jas nustato deleguotaisiais aktais pagal 27 straipsnio 9 dalį.

6 pav

Iliustracija, kaip darniojo standarto, kurio nuoroda paskelbta ir kuris apima tik pagrindinę funkciją, naudojimas lemia taikytiną atitikties vertinimo procedūrą



152. Taip yra ir tuo atveju, kai produkte su skaitmeniniais elementais yra integruota papildoma funkcija, kuri pati savaime yra kito svarbaus arba ypatingos svarbos produkto su skaitmeniniais elementais funkcija. Iš tiesų tai, ar produktas su skaitmeniniais elementais priskiriamas svarbių arba ypatingos svarbos produktų kategorijai (ir atitinkamai kokia atitikties vertinimo tvarka jam taikoma), lemia viso produkto su skaitmeniniais elementais pagrindinė funkcija, o ne atskirai vertinamos integruotų komponentų funkcijos. Pavyzdžiui, jei produkto su skaitmeniniais elementais pagrindinė funkcija atitinka I klasės svarbaus produkto su skaitmeniniais elementais pagrindinę funkciją, visam tokiam produktui taikoma I klasės svarbiems produktams su skaitmeniniais elementais nustatyta atitikties vertinimo tvarka, net jeigu į jį integruotas komponentas, kuris pats yra ypatingos svarbos produktas su skaitmeniniais elementais. Tokiais atvejais, kai gamintojas taiko darnųjį standartą, apimantį su to produkto pagrindine funkcija susijusią riziką, jis gali taikyti vidaus kontrolės procedūrą.

63 pavyzdys. Aparatinės įrangos produkto su skaitmeniniais elementais pagrindinė funkcija yra maršruto parinktuvo, apibūdinto Įgyvendinimo reglamento (ES) 2025/2392 I priedo 12 punkte, funkcija. Šis produktas su skaitmeniniais elementais taip pat turi papildomų funkcijų, įskaitant užkardos funkcijas, nes jame integruotas užkardos komponentas. Gamintojas atlieka viso produkto su skaitmeniniais elementais rizikos vertinimą, apimantį tiek maršruto parinktuvo pagrindinę funkciją, tiek užkardos funkciją. Jis taiko darnųjį standartą, apimantį su maršruto parinktuvo pagrindine funkcija susijusią riziką, ir papildomas priemones, skirtas papildomų funkcijų keliamai rizikai valdyti. Pavyzdžiui, gamintojas gali taikyti užkardoms skirtą darnųjį standartą, kad būtų aprėpiama su užkardos funkcijomis susijusi rizika. Viso produkto su skaitmeniniais elementais, įskaitant užkardos funkciją, atitikties vertinimui gamintojas gali taikyti vidaus kontrolės procedūrą.

6.3. Atitikties prezumpcijos aspektai

153. KAA 27 straipsnio 1 dalyje nustatyta, kad produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai, atitinkantys darniuosius standartus arba jų dalis, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje* (ES OL), laikomi atitinkančiais tuos KAA esminius reikalavimus, kuriuos tie standartai arba jų dalys apima ([26]). Pagal

([26]) Kaip aiškiai nurodyta Mėlynojo vadovo 4.1.2.2 skirsnyje, „[s]u rizika susijusiuose derinamuosiuose teisės aktuose [...] gamintojai visada, net ir kai remiasi darniaisiais standartais, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje* oficialiajame leidinyje, tebėra visiškai atsakingi už visos su savo gaminiu susijusios rizikos vertinimą siekiant nustatyti, kurie esminiai (arba kiti) reikalavimai svarbūs. Po šio vertinimo gamintojas gali pasirinkti taikyti darniuosiuose standartuose, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje* oficialiajame leidinyje, pateiktas techninės specifikacijas „rizikos mažinimo priemonėms“, kurios nustatytos darniuosiuose standartuose, įgyvendinti.“

27 straipsnio 5 dalį tokia pati atitikties prezumpcija taikoma produktams su skaitmeniniais elementais ir gamintojo įdiegtiems procesams, atitinkantiems Komisijos įgyvendinimo aktais priimtas bendrąsias specifikacijas. 27 straipsnio 8 dalyje nustatyta atitikties prezumpcija taikoma produktams su skaitmeniniais elementais ir gamintojo įdiegtiems procesams, dėl kurių pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamentą (ES) 2019/881, išduotas ES atitikties pareiškimas arba sertifikatas, jeigu tai nustatyta pagal 27 straipsnio 9 dalį priimtais deleguotaisiais aktais ([27]).

154. Todėl, kai gamintojas taiko darnųjį standartą, kurio nuoroda paskelbta ES OL, jam taikoma atitikties prezumpcija dėl to standarto apimamos rizikos. Taip gali būti, pavyzdžiui, kai atitinkamas darnusis standartas apima visą su produkto su skaitmeniniais elementais pagrindine funkcija susijusią riziką ir produktas neturi papildomų funkcijų, keliančių kibernetinio saugumo riziką. Pavyzdžiui, tikimasi, kad maršruto parinktuvams skirtas darnusis standartas apims bent su šių produktų su skaitmeniniais elementais pagrindine funkcija susijusią riziką. Jeigu toks produktas neturi papildomų funkcijų arba jeigu šios papildomos funkcijos nekelia rizikos, kurios standartas neapima, produktui su skaitmeniniais elementais gali būti taikoma atitikties prezumpcija.

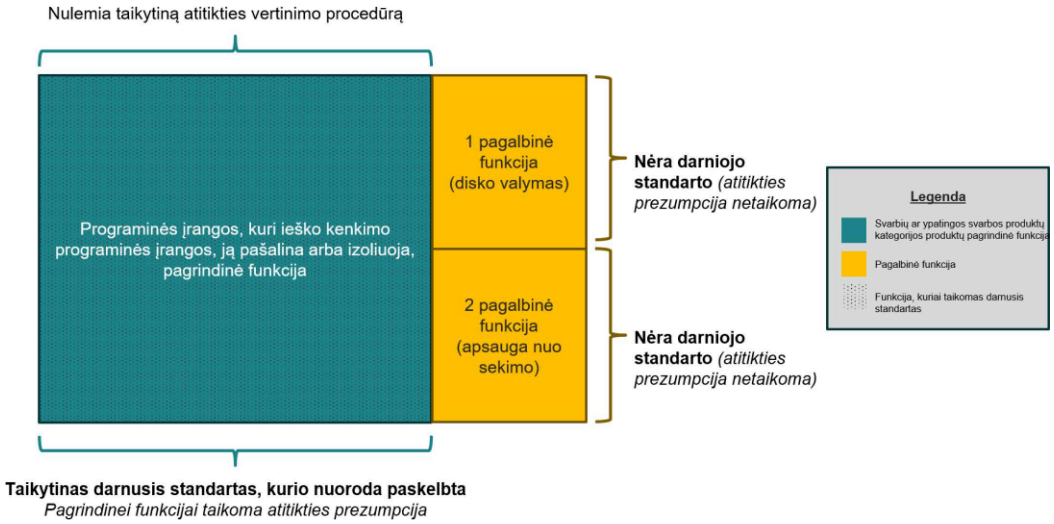
155. 151 ir 152 punktuose aptartais atvejais gamintojas gali taikyti vidaus kontrolės procedūrą, nes darnusis standartas apima su produkto su skaitmeniniais elementais pagrindine funkcija susijusią riziką. Tačiau tuose pavyzdžiuose aprašytų produktų su skaitmeniniais elementais aprėptis gali būti platesnė už darniųjų standartų taikymo sritį, o papildomos funkcijos gali kelti kibernetinio saugumo riziką, kurios toks darnusis standartas neapima. Todėl tokioms papildomoms funkcijoms atitikties prezumpcija gali būti netaikoma.

64 pavyzdys. Antivirusinės programinės įrangos pagrindinė funkcija yra ieškoti kenkimo programinės įrangos, ją pašalinti arba izoliuoti, o su šia pagrindine funkcija susijusią riziką apima darnusis standartas. Šis produktas su skaitmeniniais elementais taip pat turi papildomų funkcijų, būtent disko valymo funkciją ir apsaugos nuo sekimo funkciją, kuri apsaugo naudotoją, kai jis naršo internete, tačiau su šiomis funkcijomis susijusios rizikos darnusis standartas neapima. Jeigu darnusis standartas taikomas, gamintojas atitikties vertinimui gali taikyti vidaus kontrolės procedūrą. Atitikties prezumpcija jam bus taikoma dėl su produkto pagrindine funkcija susijusios rizikos, tačiau ne dėl su papildomomis funkcijomis susijusios rizikos.

([27]) Kaip nurodyta pirmiau, siekiant glaustumo, likusioje šio skirsnio dalyje minimi tik darnieji standartai, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*. Tačiau tos pačios gairės taip pat taikomos bendrosioms specifikacijoms ir Europos kibernetinio saugumo sertifikavimo schemoms.

7 pav

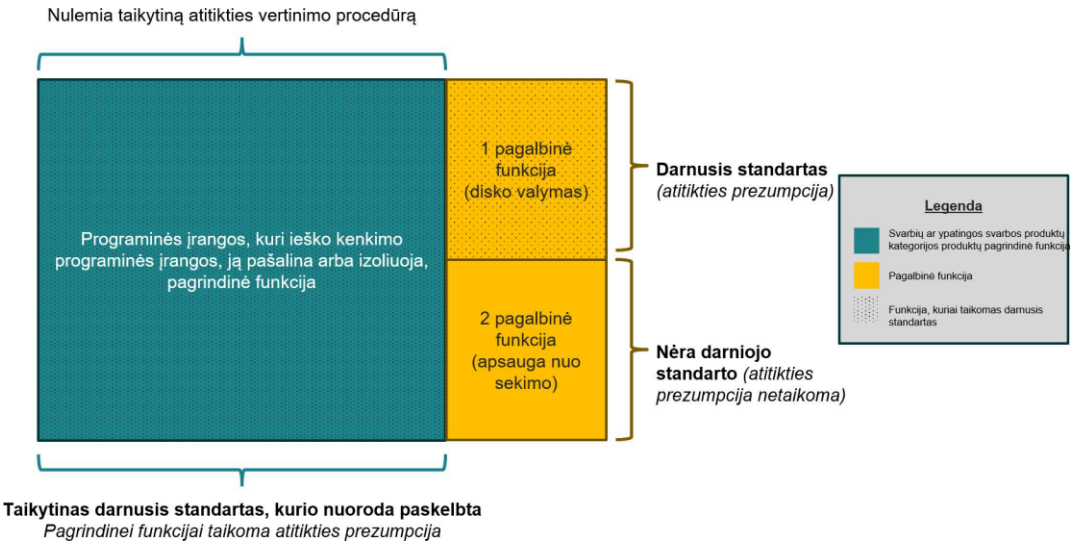
Darnusis standartas suteikia atitikties prezumpciją dėl pagrindinės funkcijos, nes apima visą su ta pagrindine funkcija susijusią riziką, tačiau nesuteikia atitikties prezumpcijos dėl pagalbinių funkcijų



65 pavyzdys. Pagal tokį patį scenarijų kaip pirmesniame pavyzdyje darnusis standartas dabar yra atnaujintas taip, kad apimtų ir su viena iš papildomų funkcijų, būtent disko valymo funkcija, susijusią riziką, tačiau neapima su kita papildoma (t. y. apsaugos nuo sekimo) funkcija susijusios rizikos. Jeigu darnusis standartas taikomas, gamintojas atitikties vertinimui gali taikyti vidaus kontrolės procedūrą. Atitikties prezumpcija jam taikoma dėl su to produkto pagrindine funkcija ir disko valymo funkcija susijusios rizikos, tačiau ne dėl su apsaugos nuo sekimo funkcija susijusios rizikos.

8 pav

Darnusis standartas suteikia atitikties prezumpciją dėl pagrindinės funkcijos ir 1 pagalbinės funkcijos, nes apima visą su šiomis dviem funkcijomis susijusią riziką, tačiau nesuteikia atitikties prezumpcijos dėl 2 pagalbinės funkcijos



7. **KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS IR PRODUKTŲ SU SKAITMENINIAIS ELEMENTAIS BEI KOMPONENTŲ INTEGRAVIMAS**

7.1. **Kibernetinio saugumo rizikos vertinimas ir valdymas**

156. Atlikdami KAA 13 straipsnio 2 dalyje numatytą kibernetinio saugumo rizikos vertinimą gamintojai privalo nustatyti atitinkamą riziką ir įvertinti galimą jos poveikį produktui su skaitmeniniais elementais. Gamintojai taip pat turi įgyvendinti tinkamas priemones šiai rizikai valdyti pagal I priede nustatytus esminius reikalavimus.

157. Organizacijos rizikos valdymo srityje rizika paprastai vertinama pagal priimtinumo kriterijus, nustatytus atsižvelgiant į organizacijos vidaus tikslus arba jos norimą prisiimti riziką. Tačiau pagal KAA liekamoji kibernetinio saugumo rizika turėtų būti vertinama atsižvelgiant į reikalavimą, kad būtų užtikrintas tinkamas rinkai pateikiamo produkto su skaitmeniniais elementais kibernetinio saugumo lygis, turint omenyje jo numatytąją paskirtį ir pagrįstai numatomą naudojimą.

158. Todėl nustatant, ar rizika tinkamai valdoma, gamintojo vidaus rizikos tolerancija, komercinė strategija ar vien sąnaudų aspektai nėra reikšmingi. 13 straipsnio 2 ir 3 dalių taikymo tikslais gamintojai turi gebėti nustatyti, ar nustatyta kibernetinio saugumo rizika yra pakankamai suvaldyta įgyvendinus I priedo I dalyje nustatytus esminius reikalavimus, atsižvelgiant į numatytąją paskirtį, pagrįstai numatomą naudojimą ir naudojimo sąlygas, įskaitant, kai aktualu, veiklos aplinką (pavyzdžiui, numatomus produkto su skaitmeniniais elementais naudotojus) ir saugotinus išteklius, taip pat atsižvelgiant į laikotarpį, kuriuo produktą su skaitmeniniais elementais numatoma naudoti.

159. Liekamoji kibernetinio saugumo rizika yra neišvengiamas rizikos vertinimo ir rizikos valdymo rezultatas. Pripažįstama, kad praktiškai kibernetinio saugumo rizikos visiškai pašalinti neįmanoma. Tačiau liekamosios rizikos buvimas nereiškia, kad gamintojas savo nuožiūra gali pripažinti priimtina bet kokią riziką. Produktas su skaitmeniniais elementais gali būti pateiktas rinkai tik tuo atveju, kai, ėmusis tinkamų priemonių, liekamoji rizika yra pakankamai suvaldyta įgyvendinant esminius reikalavimus ir atsižvelgiant į produkto su skaitmeniniais elementais numatytąją paskirtį bei pagrįstai numatomą naudojimą.

160. Pagal 13 straipsnio 3 dalį, nustačius kibernetinio saugumo riziką, gamintojai privalo ją valdyti tinkamomis priemonėmis, įskaitant produkto lygmeniu taikomas priemones. Atsižvelgiant į aplinkybes, tai gali reikšti, pavyzdžiui, atakos pažeidžiamos srities mažinimą, techninių apsaugos priemonių įgyvendinimą, funkcijų ribojimą ar pritaikymą arba tikslesnį produkto su skaitmeniniais elementais numatytosios paskirties apibrėžimą. Gamintojai taip pat gali imtis priemonių, darančių įtaką pagrįstai numatomam produkto su skaitmeniniais elementais naudojimui, pavyzdžiui, informuoti apie riziką, teikti naudotojams gaires arba atitinkamai projektuoti naudotojo sąsają, kad naudotojų elgsena būtų orientuota į saugų produkto naudojimą.

161. KAA nenumatyta galimybė perkelti kibernetinio saugumo riziką ar atsakomybę naudotojams arba trečiosioms šalims siekiant kompensuoti produkto projektavimo trūkumus ar pateisinti tai, kad kibernetinio saugumo rizika paliekama nesuvaldyta. Pareiga pateikti rinkai saugų produktą su skaitmeniniais elementais ir įrodyti jo atitiktį esminiams reikalavimams tenka gamintojui.

162. Naudotojams teikiama informacija ir instrukcijos gali būti naudojamos siekiant užtikrinti saugų produkto su skaitmeniniais elementais diegimą ir naudojimą, įskaitant atvejus, kai gamintojas yra nusprendęs apriboti to produkto numatytąją paskirtį, nustatydamas, kad jis skirtas naudoti tik patikimoje aplinkoje, taip pat informuoti naudotojus apie liekamąją riziką; tokia informacija turi būti pateikiama produkto su skaitmeniniais elementais pobūdį atitinkančiu ir numatomiems jo naudotojams pritaikytu būdu.

66 pavyzdys. Gamintojas sukuria pramoninį jutiklį, skirtą naudoti patikimoje aplinkoje. Kad jutiklis tinkamai atliktų savo funkciją, gamintojas neįgyvendina priemonių, skirtų pačiam jutikliui nuo fizinių išpuolių apsaugoti. Siekdamas sumažinti su tuo susijusią riziką, nustatytą atliekant rizikos vertinimą, gamintojas apriboja jutiklio numatytąją paskirtį – nustato, kad jis gali būti naudojamas tik patikimoje aplinkoje, kurioje užkertamas kelias neleistinai fizinei prieigai prie produkto su skaitmeniniais elementais. Naudotojams skirtoje informacijoje ir instrukcijose produkto su skaitmeniniais elementais pobūdį atitinkančiu ir numatomiems jo naudotojams pritaikytu būdu pateikiama aiški informacija apie šiuos jutiklio naudojimo apribojimus.

67 pavyzdys. Gamintojas sukuria profesionaliam naudojimui skirtą taikomąją programinę įrangą, naudojamą valdomuose staliniuose ir mobiliuosiuose įrenginiuose. Taikomoji programa tvarko įrenginyje saugomus neskelbtinus duomenis ir naudotojų sukurtą turinį. Atlikdamas rizikos vertinimą gamintojas nustato neteisėtos prieigos prie tokių duomenų, jei jie įrenginyje saugomi atviruoju tekstu, riziką. Užuot sukūręs ir pačioje taikomojoje programoje įdiegęs nuosavybinį šifravimo mechanizmą, gamintojas nusprendžia naudotis operacinėje sistemoje, kurioje taikomoji programa skirta veikti, integruotomis šifravimo ir raktų valdymo funkcijomis, nes operacinėje sistemoje integruotos kriptografinės paslaugos yra brandžios ir reguliariai prižiūrimos.

163. Jeigu atliekant kibernetinio saugumo rizikos vertinimą nustatoma rizika, kurios neįmanoma pakankamai suvaldyti tinkamomis priemonėmis, siekiant užtikrinti atitiktį KAA reikalavimams gali tekti pakeisti produkto su skaitmeniniais elementais projektą, funkcijas arba numatytąją paskirtį. Vien su sąnaudomis ar komerciniu perspektyvumu susiję argumentai nėra pakankamas pagrindas nevaldyti tokios rizikos, jeigu dėl to produktas su skaitmeniniais elementais neatitiktų esminių reikalavimų.

7.2. **Produktų su skaitmeniniais elementais projektavimas, kūrimas ir gamyba užtikrinant riziką atitinkantį jų kibernetinio saugumo lygį**

164. KAA I priedo I dalies 1 punkte nurodytame esminiame kibernetinio saugumo reikalavime nustatyta, kad produktai su skaitmeniniais elementais turi būti projektuojami, kuriami ir gaminami taip, kad būtų užtikrintas riziką atitinkantis jų kibernetinio saugumo lygis.

165. Šiuo esminiu reikalavimu siekiama valdyti visą kibernetinio saugumo riziką, nustatytą atliekant kibernetinio saugumo rizikos vertinimą. Visų pirma tai apima kibernetinio saugumo riziką, kuri nėra kitaip tinkamai suvaldyta įgyvendinant kitus I priedo I dalyje, išskyrus 1 punktą, nustatytus esminius reikalavimus. Šis esminis reikalavimas skiriasi nuo teisinės pareigos atlikti kibernetinio saugumo rizikos vertinimą pagal 13 straipsnio 2 dalį.

166. Jeigu visa atitinkama su produktu su skaitmeniniais elementais susijusi kibernetinio saugumo rizika yra suvaldyta įgyvendinus tinkamas priemones, skirtas taikytiniems esminiams reikalavimams, išskyrus 1 punkte nurodytą reikalavimą, įvykdyti, laikoma, kad I priedo I dalies 1 punkte nurodytas esminis reikalavimas yra įvykdytas. Ir, priešingai, jeigu atliekant kibernetinio saugumo rizikos vertinimą nustatoma papildoma rizika, kuri tokiomis priemonėmis nėra visiškai suvaldyta, gamintojai privalo įgyvendinti tinkamas priemones produkto su skaitmeniniais elementais lygmeniu tai rizikai valdyti, kad būtų laikomasi I priedo I dalies 1 punkte nurodyto esminio reikalavimo. Tikimasi, kad praktikoje laikantis kitų esminių reikalavimų daugeliu atvejų bus užtikrintas ir šio reikalavimo laikymasis.

7.3. **Rizikos vertinimas ir išsamus patikrinimas, susiję su išorine priklausomybe ir integruotais komponentais**

167. KAA gamintojams nustatomos dvi atskiros, tačiau viena kitą papildančios pareigos, susijusios su kibernetinio saugumo rizikos valdymu. Pirma, pagal 13 straipsnio 2 dalį gamintojai privalo atlikti paties produkto su skaitmeniniais elementais kibernetinio saugumo rizikos vertinimą. Antra, 13 straipsnio 5 dalyje nustatyta pareiga atlikti išsamų integruotų komponentų patikrinimą. Šiomis abiem pareigomis siekiama užtikrinti, kad produktas su skaitmeniniais elementais išliktų saugus, taip pat tais atvejais, kai jis priklauso nuo nuotolinio duomenų tvarkymo sprendinių, nuotolinių paslaugų arba trečiųjų šalių programinės ar aparatinės įrangos komponentų.

168. Kibernetinio saugumo rizikos vertinimas apima atitinkamos rizikos, galinčios daryti poveikį produktui su skaitmeniniais elementais, (įskaitant riziką, kurios šaltinis yra ne pats produktas, o, pavyzdžiui, išoriniai tinklai, aplinkos veiksniai ar kiti išorės aspektai, kurie gali paveikti produktą su skaitmeniniais elementais arba nuo kurių tas produktas priklauso) nustatymą ir valdymą. Kalbant apie tokią išorinę riziką, KAA nereikalaujama, kad gamintojai kontroliuotų ar valdytų išorinę aplinką. Gamintojai turi nustatyti tokią riziką ir ją mažinti projektuodami bei kurdami patį produktą su skaitmeniniais elementais. Tam reikia įgyvendinti I priedo I dalyje nustatytus atitinkamus esminius reikalavimus ir, kai būtina, pateikti naudotojams informaciją bei instrukcijas apie su integravimu ar diegimu susijusią riziką.

169. Pavyzdžiui, gamintojas gali nustatyti riziką, kad gaminiui veikiant leidimo neturintys asmenys gali gauti prieigą prie galinių sistemų, kurios nėra paties produkto su skaitmeniniais elementais dalis, ir mėginti siųsti produktui su skaitmeniniais elementais kenkimo komandas. Tokios galinės sistemos, jeigu jų nesuprojektavo ir nesukūrė pats gamintojas ar jos nebuvo sukurtos jo atsakomybe arba jeigu jos nepalaiko kurios nors produkto su skaitmeniniais elementais funkcijos, nelaikomos nuotolinio duomenų tvarkymo sprendiniais, todėl nepatenka į produkto su skaitmeniniais elementais aprėptį pagal KAA. Vis dėlto pagal KAA gamintojas privalo valdyti jų galimą riziką produkto lygmens priemonėmis, pavyzdžiui, reikalaudamas nuotolinių komandų kriptografinio tapatumo nustatymo, tikrindamas konfigūracijos pakeitimų vientisumą arba generuodamas su saugumu susijusius žurnalų įrašus ar įspėjimus, kai nustatomas neįprastas elgesys. Panašiai, jei gamintojas nustato riziką, kylančią dėl tokios išorinės paslaugos nepasiekiamumo, pavyzdžiui, nutrūkus elektros energijos tiekimui ar sutrikus infrastruktūrai, pagal KAA gali būti reikalaujama tokios kibernetinio saugumo rizikos mažinimo priemones taikyti produkto lygmeniu, pavyzdžiui, užtikrinti, kad dėl paslaugos sutrikimo produktas su skaitmeniniais elementais nepereitų į nesaugią būseną. KAA reglamentuojama, kaip tokiais atvejais produktas su skaitmeniniais elementais reaguoja į šią išorinę riziką; jame nenustatoma pareigų dėl galinės sistemos infrastruktūros organizavimo, darbuotojų skyrimo ar eksploatavimo ir tokia infrastruktūra nelaikoma produkto su skaitmeniniais elementais dalimi.

170. Išsamus patikrinimas yra susijęs su elementais, kurie yra paties produkto su skaitmeniniais elementais dalis, visų pirma su trečiosios šalies pateiktais integruotais programinės ar aparatinės įrangos komponentais. Gamintojai privalo imtis tinkamų priemonių užtikrinti, kad tokie komponentai nepakenktų produkto su skaitmeniniais elementais atitikčiai esminiams reikalavimams. Tai galima pasiekti tik nustačius, kokie reikalavimai keliami produkto su skaitmeniniais elementais komponentams, kad būtų pasiekti jo kibernetinio saugumo tikslai, ir rizika grindžiamu būdu patikrinus, ar tie komponentai atitinka produkto poreikius, kaip nurodyta ir 34 konstatuojamojoje dalyje.

171. Atsižvelgdamas į savo atliktą kibernetinio saugumo rizikos vertinimą, gamintojas turi nustatyti reikalavimus, kuriuos turėtų atitikti integruotas komponentas. Pavyzdžiui, jeigu produktas su skaitmeniniais elementais priklauso nuo komponento teikiamų kriptografinių funkcijų, naujinimo mechanizmų ar saugaus ryšio funkcijų, gamintojas, atlikdamas išsamų patikrinimą, privalo nustatyti šiuos poreikius ir patikrinti, ar komponentas juos atitinka. Tam pagrįsti gali būti naudojami iš komponento gamintojo gauti dokumentai, pavyzdžiui, techninės specifikacijos, saugumo dokumentai arba atitinkami atitikties ar saugumo užtikrinimo dokumentai. Kai tinkama, gamintojas taip pat gali atlikti bandymus, kad patikrintų, ar šie komponentai tinkamai atlieka atitinkamas funkcijas. Nors išsamus patikrinimas yra atskira teisinė pareiga, jis padeda gamintojui pagrįsti ir įrodyti viso produkto su skaitmeniniais elementais atitiktį esminiams reikalavimams.

172. Vertinant viso produkto su skaitmeniniais elementais riziką, atliekant kibernetinio saugumo rizikos vertinimą turi būti atsižvelgiama ir į produktui nepriklausančius elementus, pavyzdžiui, aplinkos veiksnius, išorinę infrastruktūrą, kitas sistemas ar tinklus, o kai aktualu, su jais susijusi rizika turi būti valdoma produkto lygmeniu taikomomis priemonėmis, kad būtų užtikrinta produkto su skaitmeniniais elementais atitiktis esminiams reikalavimams. Atliekant rizikos vertinimą taip pat turi būti atsižvelgiama į komponentus, kurie yra fiziškai ar logiškai integruoti į produktą su skaitmeniniais elementais, tačiau yra gauti iš trečiosios šalies. Vis dėlto atitikties užtikrinimo tikslais gamintojas turėtų juos vertinti kaip iš išorės tiekiamus komponentus, kurių savybės integravimo metu patikrinamos atliekant išsamų patikrinimą, nes gali būti, kad gamintojas pats jų neperprojektuoja ar iš naujo nesukuria.

173. Ta pati logika taikoma kuriant ir integruojant komponentus. Kai gamintojas funkcijas kuria pats, jis privalo tiesiogiai įgyvendinti esminius reikalavimus. Kai gamintojas integruoja kitų subjektų sukurtus komponentus, jis privalo užtikrinti, atlikdamas išsamų patikrinimą, kad tie komponentai galėtų būti naudojami taip, kad visas produktas su skaitmeniniais elementais atitiktų esminius reikalavimus. Abiem atvejais tikslas išlieka tas pats – užtikrinti, kad rinkai pateikiamas produktas su skaitmeniniais elementais pasiektų KAA reikalaujamą kibernetinio saugumo lygį, atsižvelgiant į atliekant kibernetinio saugumo rizikos vertinimą nustatytą riziką.

7.4. **Rizikos vertinimų ir atitikties dokumentų pakartotinis naudojimas produktų su skaitmeniniais elementais grupėms**

174. Gamintojai gali pateikti rinkai panašius produktus su skaitmeniniais elementais, pavyzdžiui, skirtingus tos pačios grupės produktų variantus, modelius ar konfigūracijas. Kai tokių produktų su skaitmeniniais elementais architektūra, saugumui svarbūs projektavimo sprendiniai ir numatytoji paskirtis yra tokie patys ir jiems kyla tokia pati kibernetinio saugumo rizika, pagal KAA nereikalaujama, kad rizikos vertinimo ir atitikties vertinimo tikslais gamintojai kiekvieną variantą laikytų visiškai atskiru produktu su skaitmeniniais elementais.

175. Tokiais atvejais, jeigu visi atitinkami variantai yra tinkamai įvertinti atsižvelgiant į atitinkamą riziką ir esminius reikalavimus, gamintojai gali remtis: i) vienu pagal KAA 13 straipsnio 2 dalį atliktu kibernetinio saugumo rizikos vertinimu, ii) vienu techninių dokumentų rinkiniu ir iii) viena atitikties vertinimo procedūra. Tai taip pat leidžia išduoti vieną ES atitikties deklaraciją, skirtą produktų su skaitmeniniais elementais grupei, jeigu joje aiškiai nurodomi produktų variantai, kuriems ji taikoma.

176. Lemiamas veiksnys yra tai, ar variantų skirtumai yra reikšmingi kibernetiniam saugumui. Dėl skirtumų, kurie produkto su skaitmeniniais elementais kibernetinio saugumo savybėms įtakos neturi, pavyzdžiui, spalvos, konstrukcinės formos, atmintinės talpos ar kitų su saugumu nesusijusių charakteristikų skirtumų, atskirų rizikos vertinimų ar atitikties vertinimų atlikti nereikia. Tačiau tam tikrais atvejais variantai gali skirtis taip, kad tai turėtų įtakos esminių reikalavimų įgyvendinimui, pavyzdžiui, dėl skirtingų ryšio sąsajų, programinės įrangos išteklių rinkinių, naujinimo mechanizmų ar nuotolinio junglumo. Tokiais atvejais į šiuos skirtumus turi būti atsižvelgta atliekant rizikos vertinimą ir, kai būtina, atitikties vertinimą bei rengiant techninius dokumentus.

177. Gamintojai lieka atsakingi už tai, kad rizikos vertinimas ir susiję dokumentai tiksliai atspindėtų rinkai pateikiamus produktus su skaitmeniniais elementais. Jeigu dėl naujo varianto kyla nauja kibernetinio saugumo rizika arba pasikeičia esminių reikalavimų įgyvendinimo būdas, esamas rizikos vertinimas ir atitikties dokumentai turi būti atitinkamai atnaujinti. Vienu atitikties vertinimu galima remtis tik jei produktų su skaitmeniniais elementais kibernetinio saugumo savybės nesiskiria.

8. **NUOTOLINIS DUOMENŲ TVARKYMAS**

178. KAA 3 straipsnio 1 punkte produktas su skaitmeniniais elementais apibrėžiamas kaip „programinės ar aparatinės įrangos produktas ir jo nuotolinio duomenų tvarkymo sprendiniai, įskaitant atskirai rinkai pateikiamus programinės ar aparatinės įrangos komponentus“. Atsižvelgdamas į tai, gamintojas produktą su skaitmeniniais elementais turi vertinti kaip visumą, įskaitant jo nuotolinio duomenų tvarkymo sprendinius (toliau – NDTS). Pavyzdžiui, įrodant, kad produktas su skaitmeniniais elementais atitinka I priede nustatytus esminius reikalavimus, turi būti atsižvelgiama ir į NDTS, pradedant rizikos vertinimu (13 straipsnio 2 dalis). Tas pats taikoma vertinant su gyvavimo ciklu susijusias pareigas, pavyzdžiui, pareigą pranešti apie aktyviai išnaudojamą pažeidžiamumą ir didelius incidentus (14 straipsnis).

179. Šių gairių tikslas – suteikti gamintojams papildomos pagalbos nustatant, ar jų produktas su skaitmeniniais elementais turi KAA apibrėžtus NDTS, ir paaiškinti, kaip šiuo atžvilgiu vykdyti atitikties užtikrinimo pareigas. Iš pradžių išanalizavus KAA nustatytas apibrėžtis ir konstatuojamąsias dalis, šiose gairėse bus pateikti klausimai, padėsiantys gamintojams išsiaiškinti, ar jų produktas su skaitmeniniais elementais apima NDTS (žr. *8.1* skirsnį „*Kas laikoma produkto su skaitmeniniais elementais nuotolinio duomenų tvarkymo sprendiniu?*“). Toliau bus išsamiau aptartos techninės NDTS pasekmės ir tai, kaip vertinti atitiktį KAA (žr. *8.2* skirsnį „*Nuotolinio duomenų tvarkymo sprendinių ir kliovimosi trečiųjų šalių sprendiniais praktinės ir techninės pasekmės*“).

180. KAA 3 straipsnio 2 punkte „nuotolinis duomenų tvarkymas“ iš tiesų apibrėžiamas kaip „per atstumą vykdomas duomenų tvarkymas, kuriam programinę įrangą projektuoja ir kuria gamintojas arba tai daroma jo atsakomybe, ir be kurio produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų“. Taigi NDTS apibrėžiami kaip per atstumą vykdomo duomenų tvarkymo programinės įrangos elementai (programinė įranga 3 straipsnio 4 punkte apibrėžiama kaip „elektroninės informacinės sistemos dalis, sudaryta iš kompiuterinio kodo“). Į produkto su skaitmeniniais elementais aprėptį nesiekiama įtraukti aparatinės įrangos, kuria naudojantis gali būti vykdomas nuotolinis duomenų tvarkymas.

181. 11 ir 12 konstatuojamosiose dalyse išsamiau paaiškinama, kaip ši sąvoka turėtų būti aiškinama. 11 konstatuojamojoje dalyje paaiškinama, kad nuotolinio duomenų tvarkymo sprendinių įtraukimo tikslas – užtikrinti, kad „gamintojai tinkamai apsaugotų visus tokius produktus, nepriklausomai nuo to, ar duomenys tvarkomi arba saugomi pačiame naudotojo įrenginyje, ar tai nuotoliniu būdu daro gamintojas“. Joje taip pat nurodyta, kad „reikalavimai, susiję su nuotolinio duomenų tvarkymo sprendiniais, patenkančiais į šio reglamento taikymo sritį, neapima techninių, operatyvinių ar organizacinių priemonių, kuriomis siekiama valdyti riziką, kylančią gamintojo tinklų ir informacinių sistemų kaip visumos saugumui“.

182. Taigi iš 11 konstatuojamosios dalies matyti, kad KAA reikalavimais nesiekiama apimti visos organizacijos IT infrastruktūros – jie taikomi tik tiems programinės įrangos komponentams, kurie sudaro sąlygas vykdyti duomenų tvarkymo sprendinį. Pavyzdžiui, vidaus sistemos, susijusios su paties gamintojo žmogiškaisiais ištekliais, darbo užmokesčio apskaita, ryšių su klientais valdymu, nuolatinio integravimo ar nuolatinio pristatymo (CI/CD) procesų grandinėmis ar saugumo naujinių platinimu į tinklo paribio vietas, neturėtų būti laikomos NDTS. Be to, sistemos, susijusios su audito ir bandymo (testavimo) veikla, pavyzdžiui, skverbimosi testavimu, grėsmių paieška ir vadinamuoju raudonosios komandos (etiškais įsilaužimais grindžiamu) testavimu, nepatenka į produkto su skaitmeniniais elementais sąvokos aprėptį pagal KAA. Svarbu pažymėti, kad nors veiksmingi ir reguliarūs produkto su skaitmeniniais elementais saugumo bandymai ir peržiūros yra esminis reikalavimas, nustatytas KAA I priedo II dalies 3 punkte, tai nereiškia, kad tokia veikla turi būti laikoma to produkto su skaitmeniniais elementais NDTS.

183. 12 konstatuojamojoje dalyje dėmesys sutelktas į debesijos paslaugas ir išsamiau paaiškinama, kokiomis aplinkybėmis debesijos paslaugos gali būti laikomos NDTS. Tos konstatuojamosios dalies pabaigoje primenama, kad debesijos kompiuterijos paslaugos ir debesijos paslaugų modeliai patenka į Direktyvos (ES) 2022/2555 (TIS 2 direktyvos) ([28]) taikymo sritį; joje debesijos kompiuterijos paslaugų teikėjams nustatyti kibernetinio saugumo rizikos valdymo reikalavimai. Šie reikalavimai išsamiau nustatyti Komisijos įgyvendinimo reglamentu (ES) 2024/2690 ([29]).

8.1. **Kas laikoma produkto su skaitmeniniais elementais nuotolinio duomenų tvarkymo sprendiniu?**

184. 3 straipsnio 2 punkte nustatyta nuotolinio duomenų tvarkymo apibrėžtis grindžiama trimis elementais: i) ar duomenys tvarkomi per atstumą, ii) ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų ir iii) ar programinę įrangą projektuoja ir kuria gamintojas arba tai daroma jo atsakomybe. Tolesniuose trijuose poskirsniuose kiekvienas iš šių elementų aptariamas išsamiau.

([28]) 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) (OL L 333, 2022 12 27, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) 2024 m. spalio 17 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2690, kuriuo nustatomos Direktyvos (ES) 2022/2555 taikymo taisyklės, susijusios su kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais ir išsamesniu atvejų, kuriais incidentas laikomas dideliu, apibūdinimu, skirtais DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams (OL L, 2024/2690, 2024 10 18, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Sąvoka „per atstumą“*

185. 3 straipsnio 2 punkte vartojama sąvoka „per atstumą“ yra svarbi, tačiau jos vienos nepakanka siekiant nustatyti, ar produktas su skaitmeniniais elementais apima NDTS. Be to, atsižvelgiant į sprendinių, kuriuos sąvoka „per atstumą“ gali apimti, įvairovę, išsamios šios sąvokos apibrėžties pateikti neįmanoma. Gamintojas kiekvieną atvejį turi įvertinti individualiai.

186. KAA 11 konstatuojamojoje dalyje minimi duomenys, kuriuos „nuotoliniu būdu [tvarko arba saugo] gamintojas“, priešpriešinant juos duomenims, kurie tvarkomi arba saugomi „pačiame naudotojo įrenginyje“. Nuotolinis duomenų tvarkymas paprastai vyksta už produkto su skaitmeniniais elementais naudotojo aplinkos ribų arba, profesionalaus naudotojo atveju, už organizacijos veiklos aplinkos ribų. Tačiau tai nekliudo duomenų tvarkymui taip pat vykti arti įrenginio („tinklo paribyje“). Duomenys gali būti perduodami laidiniu ryšiu (pvz., eterneto kabeliu) arba belaidžiu ryšiu (pvz., *Wi-Fi* ar *Bluetooth*). Debesijos kompiuterija, įskaitant tinklo paribio kompiuteriją, yra tipinis duomenų tvarkymo per atstumą pavyzdys. Pavyzdžiui, kai naudotojas per mobiliąją programėlę naudojasi debesija grindžiama funkcija, dalis duomenų tvarkymo vyksta debesijoje, už naudotojo aplinkos ribų.

187. Svarbu pažymėti, kad NDTS nebūtinai yra eksploatuojami trečiųjų šalių debesijos infrastruktūroje. Nuotolinis duomenų tvarkymas gamintojo patalpose esančiuose vietiniuose serveriuose taip pat gali būti laikomas NDTS. Kitaip tariant, gamintojo vietinėje infrastruktūroje ir privačioje debesijoje veikiantis sprendinys gali būti laikomas NDTS lygiai taip pat kaip viešojoje debesijoje ir už gamintojo vietinės infrastruktūros ribų veikiantis sprendinys.

188. Toliau, *8.1.2* ir *8.2* skirsniuose, pateikiami du lemiamą reikšmę turintys ir kartu užduodami klausimai, pagal kuriuos nustatoma, ar duomenų tvarkymas patenka į KAA taikymo sritį kaip nuotolinio duomenų tvarkymo sprendinys. Jeigu į abu klausimus atsakoma teigiamai, nuotolinis duomenų tvarkymas laikomas NDTS.

8.1.2. *Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų?*

189. Kaip nustatyta 3 straipsnio 2 punkte pateiktoje sąvokos „nuotolinis duomenų tvarkymas“ apibrėžtyje, tam, kad per atstumą vykdomas duomenų tvarkymas būtų laikomas NDTS, nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais turėtų negalėti atlikti vienos iš savo funkcijų. Šioje apibrėžtyje vartojamas terminas „funkcijos“ neapsiriboja produkto su skaitmeniniais elementais „pagrindine funkcija“ ar „numatytąja paskirtimi“, nes KAA toks apribojimas nenustatytas. Į KAA taikymo sritį patenka tiek funkcijos, kuriomis, naudotojo požiūriu, tiesiogiai įgyvendinama produkto su skaitmeniniais elementais numatytoji paskirtis, tiek funkcijos, kuriomis palaikomas bendras produkto veikimas.

190. Funkcijų, kurioms atlikti duomenys gali būti tvarkomi per atstumą ir be kurių produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų, pavyzdžiai: i) komandų siuntimas į įrenginį; ii) failų sinchronizavimas; iii) naudotojo prisijungimas naudotis produktu; iv) konfigūravimas (produkto su skaitmeniniais elementais individualizavimas); v) automatizuotas naujinių platinimas, įskaitant funkcijų naujinius ir saugumo pataisų diegimą; vi) tapatybės ir prieigos valdymas.

191. Kai kuriais atvejais naudotojas tą pačią funkciją gali atlikti tiek nuotoliniu, tiek rankiniu būdu (pvz., įjungti ar išjungti elektros lemputę naudodamas programėlę arba rankiniu būdu). Tokios pasirinkimo galimybės buvimas nereiškia, kad su nuotoliniu tos funkcijos atlikimu susijęs duomenų tvarkymas negali būti laikomas NDTS. Galimybė atlikti šią funkciją nuotoliniu būdu taip pat laikoma viena iš produkto su skaitmeniniais elementais siūlomų funkcijų.

192. Ir, priešingai, kai nesant tam tikro duomenų tvarkymo produktas su skaitmeniniais elementais vis vien gali atlikti visas savo funkcijas, toks duomenų tvarkymas nelaikomas NDTS pagal KAA. Tai apima, pavyzdžiui, nuotolinę telemetrijos duomenų, renkamų tik statistikos arba produkto būsimo tobulinimo tikslais, analizę.

193. Vis dėlto net ir tais atvejais, kai duomenų tvarkymas nepalaiko jokios produkto su skaitmeniniais elementais funkcijos, gamintojams atliekant kibernetinio saugumo rizikos vertinimą gali reikėti įvertinti, ar tie nuotoliniai komponentai nekelia rizikos produktui su skaitmeniniais elementais (pvz., atsižvelgiant į produkto veikimo aplinką), ir atitinkamai tą riziką sumažinti (pvz., taikant rizikos mažinimo priemones produkto lygmeniu).

194. Saityno svetainės yra specifinis atvejis, kurį reikia išaiškinti išsamiau, kaip paaiškinta ir *2.1* skirsnyje „*Pateikimas rinkai*“. Svetainės nepatenka į NDTS apimtį, jeigu jos nepalaiko jokios produkto su skaitmeniniais elementais funkcijos, kaip paaiškinta KAA 11 konstatuojamojoje dalyje. Vien to, kad svetainėje pateikiama informacija apie produktą su skaitmeniniais elementais, nepakanka, kad ji būtų laikoma patenkančia į NDTS aprėptį, net jeigu produktas nukreipia į tokią svetainę. Pavyzdžiui, naudotojų nukreipimas į išorinį tinklalapį, kuriame jiems pateikiama informacija ir instrukcijos, nėra NDTS. Ir, priešingai, svetainė gali patekti į NDTS aprėptį, jeigu ji sudaro sąlygas atlikti produkto su skaitmeniniais elementais funkciją arba ją palaiko. Pavyzdžiui, tapatumo nustatymo portalas, kuriame išduodami kredencialai arba prieigos raktai, kurių reikia produktui su skaitmeniniais elementais veikti, būtų laikomas NDTS (jeigu yra atitiktis ir kitiems apibrėžtyje nustatytiems kriterijams).

8.1.3. *Ar programinę įrangą projektavo ir kūrė gamintojas arba tai buvo daroma jo atsakomybe?*

195. KAA 3 straipsnio 2 punkte pateiktoje „nuotolinio duomenų tvarkymo“ apibrėžtyje taip pat nustatyta, kad tokio per atstumą vykdomo duomenų tvarkymo programinę įrangą turi projektuoti ir kurti gamintojas arba tai turi būti daroma jo atsakomybe. Nuotolinis duomenų tvarkymas, kurio procesą visą suprojektavo ir sukūrė gamintojas (savo organizacijos viduje), savaime galėtų būti laikomas NDTS. Tas pats būtų taikoma ir tais atvejais, kai gamintojas sprendinio projektavimui ir kūrimui pasitelkia išorės paslaugų teikėją (t. y. kai sprendinys kuriamas „jo atsakomybe“). Formuluotė „gamintojo atsakomybe“ reiškia specialiai gamintojui pritaikytus nuotolinio duomenų tvarkymo sprendinius. Tai atvejai, kai gamintojas ne vien licencijuoja jau esamą produktą su skaitmeniniais elementais ar paslaugą, kurią paslaugų teikėjas siūlo savo klientams, arba tik nežymiai pakeistą tokio produkto ar paslaugos versiją. Formuluotė „gamintojo atsakomybe“ reiškia, kad programinė įranga sukurta tik paties gamintojo arba jo vardu, remiantis jo pateiktais projektiniais sprendiniais ir specifikacijomis.

196. Siekiant suprasti NDTS, klausimas, kas tą sprendinį eksploatuoja, nėra lemiamas veiksnys, nes KAA nustatytoje apibrėžtyje nurodomas tik NDTS projektavimas ir kūrimas. Tai atitinka KAA požiūrį, pagal kurį reikalavimai ir pareigos nustatomi gamintojams, o ne produkto su skaitmeniniais elementais eksploatavimui. Jeigu gamintojai projektuoja ir kuria sprendinius, kuriuos vėliau eksploatuoja trečioji šalis, jie ir toliau atsako už produkto su skaitmeniniais elementais, kurį jie pateikia rinkai, atitiktį KAA esminiams reikalavimams.

197. Būtina skirti atvejus, kai projektuoja ir kuria gamintojas (arba tai daroma jo atsakomybe), nuo atvejų, kai kliaujamasi trečiųjų šalių sprendiniais, kurių gamintojas neprojektavo ir nekūrė (ir kurie nebuvo projektuojami ar kuriami jo atsakomybe). Kaip pavyzdį naudinga panagrinėti dažniausiai naudojamus debesijos paslaugų modelius, pagal kuriuos naudotojui suteikiama skirtingo lygio kontrolė ir kurie taip pat nurodyti KAA 12 konstatuojamojoje dalyje, t. y. paslauginę programinę įrangą (angl. *Software as a Service*, toliau – SaaS), paslauginę platformą (*Platform as a Service*, toliau – PaaS) ir paslauginę infrastruktūrą (*Infrastructure as a Service*, toliau – IaaS).

198. Trečiosios šalies IaaS sprendinio atveju gamintojas nevaldo ir nekontroliuoja pagrindinių fizinių ir virtualių išteklių (pvz., pagrindinės aparatinės įrangos ir debesijos paslaugų teikėjo sistemos prižiūryklės), tačiau naudodamasis tais ištekliais gali diegti ir naudoti savo pasirinktą programinę įrangą, pavyzdžiui, operacines sistemas ir taikomąsias programas. Tokią programinę įrangą projektuoja ir kuria pats gamintojas arba tai daroma jo atsakomybe, todėl ji gali būti laikoma NDTS (jeigu ji atitinka ir kitus apibrėžties elementus).

199. Trečiosios šalies PaaS sprendinio atveju gamintojas, naudodamas debesijos paslaugų teikėjo suteikiamas programavimo kalbas ir vykdymo aplinką, įdiegia savo sukurtą arba įsigytą taikomąją programą ir integruoja ją į savo produktą su skaitmeniniais elementais. Gamintojas kontroliuoja taikomąją programą ir galbūt tam tikrus vykdymo aplinkos konfigūracijos parametrus. Taigi taikomąją programą projektuoja ir kuria gamintojas arba tai daroma jo atsakomybe, todėl ji gali būti laikoma NDTS (jeigu ji atitinka ir kitus apibrėžties elementus).

200. Trečiosios šalies SaaS sprendinio atveju SaaS teikėjas gamintojui siūlo visiškai sukurtą taikomąją programą, kuri yra integruojama į gamintojo produktą su skaitmeniniais elementais. Gamintojo galimybės valdyti konkrečiam naudotojui skirtus taikomosios programos konfigūracijos parametrus yra ribotos. Todėl gamintojas tokios taikomosios programos neprojektuoja ir nekuria ir tai nėra daroma jo atsakomybe.

201. Vis dėlto, kai tam tikri elementai nelaikomi NDTS (pvz., sistemos prižiūryklė trečiosios šalies IaaS infrastruktūros atveju, operacinė sistema trečiosios šalies PaaS sprendinio atveju arba trečiosios šalies SaaS taikomoji programa), tačiau yra integruoti į produktą su skaitmeniniais elementais taip, kad daro poveikį jo saugumui, tokie sprendiniai turėtų būti vertinami panašiai kaip trečiųjų šalių suteikti komponentai. Gamintojas privalo nustatyti ir įvertinti su tokių elementų integravimu susijusią riziką ir ją valdyti įgyvendindamas esminius reikalavimus pačiame produkte su skaitmeniniais elementais. Kai tinkama, tam gali būti pasitelkiamos saugumo funkcijos, kurias debesijos paslaugų teikėjas suteikia pagal savo bendros atsakomybės modelį, jeigu gamintojas tas funkcijas naudoja arba sukonfigūruoja taip, kad būtų valdoma nustatyta rizika. Be to, tikimasi, kad gamintojas tokių komponentų saugumo atžvilgiu atliks pareigą, panašią į 13 straipsnio 5 dalyje nurodytą pareigą atlikti išsamų patikrinimą, proporcingai tai rizikai, kurią nuotolinis sprendinys kelia produkto su skaitmeniniais elementais saugumui.

202. Taigi galima apibendrinti taip:

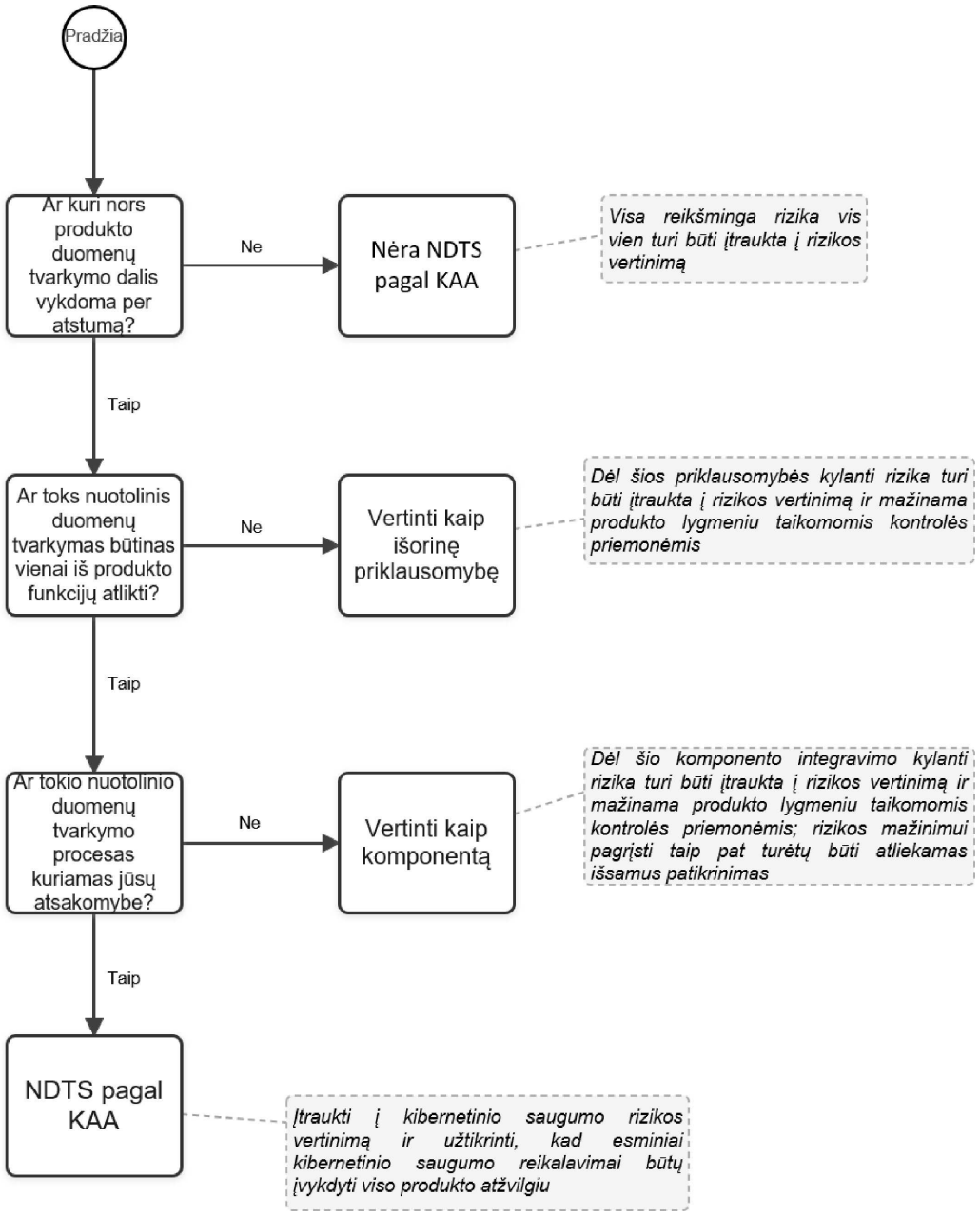
a) Kad duomenų tvarkymas būtų laikomas NDTS, į abu *8.1.2* skirsnyje *„Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų?“* ir *8.1.3* skirsnyje *„Ar programinę įrangą projektavo ir kūrė gamintojas arba tai buvo daroma jo atsakomybe?“* pateiktus klausimus turi būti atsakyta teigiamai.

b) Jeigu į *8.1.2* skirsnyje *„Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų?“* pateiktą klausimą atsakoma neigiamai, gamintojai atlikdami rizikos vertinimą turėtų įvertinti riziką, kylančią dėl tokio duomenų tvarkymo.

c) Jeigu į *8.1.2* skirsnyje *„Ar nesant tokio duomenų tvarkymo produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų?“* pateiktą klausimą atsakoma teigiamai, tačiau į *8.1.3* skirsnyje *„Ar programinę įrangą projektavo ir kūrė gamintojas arba tai buvo daroma jo atsakomybe?“* pateiktą klausimą atsakoma neigiamai, gamintojai tokį trečiosios šalies sprendinį turėtų vertinti kaip komponentą. Atlikdami rizikos vertinimą gamintojai turėtų įvertinti dėl tokio sprendinio integravimo kylančią riziką ir imtis atitinkamų jos mažinimo priemonių. Be to, gamintojai turėtų atlikti išsamų patikrinimą.

9 pav

Stilizuota schema, skirta nustatyti, ar produktas su skaitmeniniais elementais apima NDTS



8.2. Nuotolinio duomenų tvarkymo sprendinių ir kliovimosi trečiųjų šalių sprendiniais praktinės ir techninės pasekmės

203. KAA vadovaujamasi rizika grindžiamu požiūriu, įtvirtintu 13 straipsnio 2 ir 3 dalyse, taip pat I priedo I dalies pirmajame esminiame reikalavime, pagal kurį „[p]roduktai su skaitmeniniais elementais projektuojami, kuriami ir gaminami taip, kad, atsižvelgiant į riziką, būtų užtikrintas tinkamas kibernetinio saugumo lygis“. Todėl rizika pagrįstu požiūriu turėtų būti vadovaujamasi ir taikant KAA reikalavimus NDTS bei vertinant riziką, kylančią dėl į produktą su skaitmeniniais elementais integruotų trečiųjų šalių paslaugų.

204. Pirmiausia gamintojai turėtų: i) techniniuose dokumentuose nurodyti, kad jų produktas su skaitmeniniais elementais apima NDTS arba yra priklausomas nuo trečiųjų šalių nuotolinių sprendinių, ir ii) aprašyti tokius sprendinius. Jeigu tas pats NDTS palaiko kelis produktus su skaitmeniniais elementais, jis turi būti nurodytas kiekvieno produkto techniniuose dokumentuose. Su keliems produktams su skaitmeniniais elementais naudojamu NDTS susiję dokumentai gali būti pakartotinai naudojami atliekant skirtingų produktų atitikties vertinimus.

205. Kaip nurodyta 11 konstatuojamojoje dalyje, NDTS, kurie yra produkto su skaitmeniniais elementais dalis ir todėl patenka į produkto atitikties vertinimo aprėptį, turėtų apsiriboti tais programinės įrangos moduliais, kurie užtikrina produkto su skaitmeniniais elementais funkcionalumą, ir sąsajomis, kurias šie moduliai naudoja sąveikai su išorės paslaugomis. Tolesnį duomenų tvarkymą atliekančios galinės sistemos, su kuriomis produktas su skaitmeniniais elementais tiesiogiai nesąveikauja, nelaikomos NDTS.

206. Vis dėlto išorinė priklausomybė nuo tokių galinių sistemų išlieka ir turi būti įvertinta atliekant kibernetinio saugumo rizikos vertinimą, o jos keliama rizika turi būti sumažinta taikant priemones produkto lygmeniu. Iš tiesų gamintojo atliekamame rizikos vertinime turėtų būti atsižvelgiama į: i) su NDTS susijusią riziką, ii) riziką, susijusią su priklausomybe nuo trečiųjų šalių nuotolinių sprendinių, kuri vertinama panašiai kaip su trečiųjų šalių komponentais susijusi rizika, ir iii) su produkto aplinka (pvz., pagrindine aparatine įranga) susijusią riziką. Siekdami sumažinti šią riziką, gamintojai turėtų įgyvendinti saugumo kontrolės priemones pačiame produkte su skaitmeniniais elementais.

207. Be to, atliekant atitikties vertinimą ir (arba) vykdant su trečiųjų šalių nuotolinėmis paslaugomis susijusias išsamaus patikrinimo pareigas, gamintojo atliekamam vertinimui pagrįsti gali būti pakartotinai naudojami, be kita ko, šie atitikties ir saugumo užtikrinimo įrodymai:

a) įrodymai, kad įvykdytos Komisijos įgyvendinimo reglamente (ES) 2024/2690 nustatytos pareigos;

b) įrodymai, kad įvykdytos Reglamente (ES) 2022/2554 (SVAA) nustatytos pareigos;

c) atitikties pareiškimas arba sertifikatas, gautas pagal Europos kibernetinio saugumo sertifikavimo schemą (patvirtintą pagal Reglamentą (ES) 2019/881 – Kibernetinio saugumo aktą);

d) atitikties ISO/IEC 27017:2015 arba ISO/IEC 27001:2022 įrodymai.

208. Galiausiai, bendradarbiaudami su nuotolines paslaugas teikiančiomis trečiosiomis šalimis, gamintojai, remdamiesi savo rizikos vertinimu, turi įgyvendinti tinkamiausias saugumo priemones (o kai tinkama – jas taip pat pagrįsti paslaugų teikėjo bendros atsakomybės modeliu). Tokios rizikos mažinimo priemonės turėtų apimti gamintojų produktų su skaitmeniniais elementais saugumo kontrolės priemones ir pačių trečiųjų šalių paslaugų teikėjų taikomų saugumo priemonių patikrinimą (išsamų patikrinimą). Viena iš priemonių tokiai rizikai mažinti gali būti saugumo garantijų, įskaitant garantijas, kad paslaugų teikėjai tinkamai valdo pažeidžiamumą, įtraukimas į su paslaugas teikiančiomis trečiosiomis šalimis sudaromus susitarimus dėl paslaugų lygio (angl. *service level agreements*, SLA). Esminis nuotolines paslaugas teikiančių trečiųjų šalių teikiamų sprendinių pakeitimas neturėtų būti laikomas esminiu produkto su skaitmeniniais elementais pakeitimu, nes šie elementai nepriklauso gamintojo atsakomybei. Tačiau gamintojai raginami, kad vykdydami išsamaus patikrinimo pareigas ir siekdami tinkamai mažinti dėl naudojimosi trečiųjų šalių paslaugų teikėjų paslaugomis kylančią riziką užtikrintų, kad debesijos paslaugas teikiančios trečiosios šalys juos tinkamai informuotų apie savo sprendiniuose atliekamus pakeitimus. Remiantis tokia informacija, gamintojams gali tekti peržiūrėti savo rizikos vertinimą. Atnaujintame rizikos vertinime turėtų būti įvertinta, ar paslaugas teikiančios trečiosios šalys vis dar suteikia pakankamas kibernetinio saugumo garantijas ir ar produkto lygmeniu taikomos saugumo kontrolės priemonės tebėra tinkamos. Kai kuriais atvejais gamintojams gali tekti tokias kontrolės priemones pakeisti arba pasirinkti kitą paslaugas teikiančią trečiąją šalį.

8.3. **Nuotolinio duomenų tvarkymo sprendinių naudojimo atvejai**

Siekiant pateikti gamintojams papildomų praktinių gairių, šiame skirsnyje pateikiami keli hipotetiniai naudojimo atvejai, kuriuose aprašomi tipiniai produktai su skaitmeniniais elementais, grindžiami nuotoliniu duomenų tvarkymu, ir paaiškinama, ar toks duomenų tvarkymas laikytinas nuotolinio duomenų tvarkymo sprendiniu pagal KAA.

8.3.1. *Mobiliosios bankininkystės programėlė*

Finansų sektoriaus subjektas pateikia rinkai mobiliosios bankininkystės programėlę. Programėlės galinės sistemos, be kita ko, palaiko tapatumo nustatymą, autorizavimą, sąskaitų valdymą ir mokėjimų vykdymą. Programėlės funkcijoms palaikyti finansų sektoriaus subjektas taiko mišrią strategiją, pagal kurią naudojama tiek jo vidaus infrastruktūra, tiek trečiųjų šalių nuotoliniai sprendiniai. Tarp jų yra:

Finansų sektoriaus subjekto infrastruktūroje veikiantys ir jo sukurti sprendiniai:

— Klientas atveria mobiliosios bankininkystės programėlę ir jo tapatybė patvirtinama per bankininkystės sąsają – paties finansų sektoriaus subjekto infrastruktūroje veikiantį ir jo sukurtą sprendinį, kuris gauna programėlės užklausas ir pateikia atitinkamus atsakymus. Bankininkystės sąsaja patikrina kliento tapatybę pateikdama užklausą sąskaitų valdymo sistemai ir suteikia prieigą prie programėlės.

— Klientas inicijuoja pervedimą naudodamasis programėle. Programėlė perduoda nurodymą bankininkystės sąsajai, o ši pateikia atitinkamą užklausą apskaitos registro sistemai.

— Sąskaitų valdymo sistema ir apskaitos registro sistema, kurios abi veikia paties finansų subjekto infrastruktūroje, tačiau yra logiškai atskirtos nuo bankininkystės sąsajos, užregistruoja operaciją.

— Apskaitos registro sistema grąžina operacijos būsenos duomenis bankininkystės sąsajai, o ši pateikia rezultatą klientui.

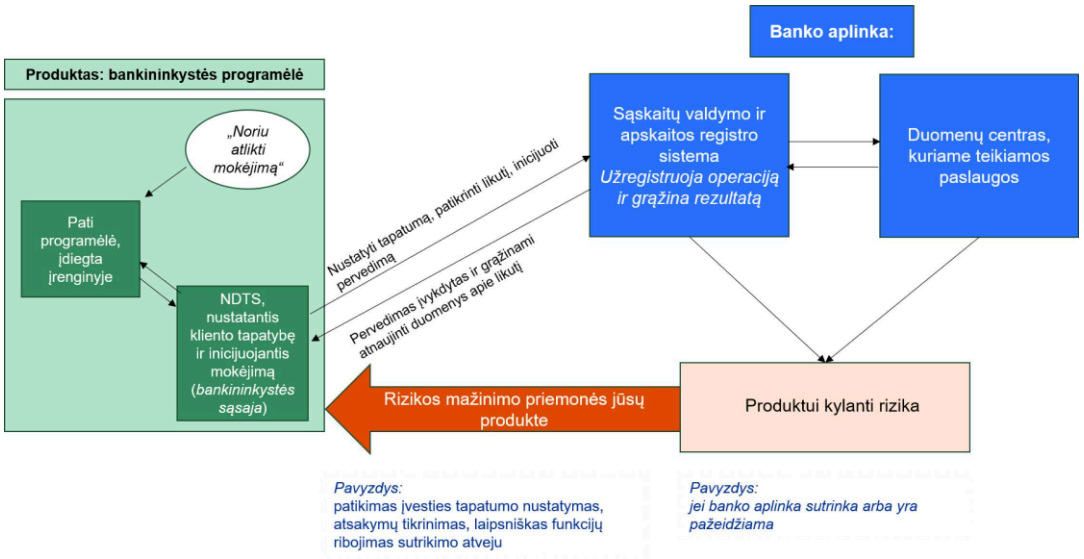
Poveikis vertinant NDTS:

— Bankininkystės sąsaja yra būtina, kad programėlė galėtų atlikti savo funkcijas, t. y. patvirtinti kliento tapatybę, perduoti kliento nurodymus, įskaitant mokėjimo ir pervedimo nurodymus, ir grąžinti jų vykdymo būsenos duomenis. Bankininkystės sąsaja projektuojama ir kuriama gamintojo atsakomybe. Kadangi į abu pirmesniuose skirsniuose pateiktus klausimus atsakoma teigiamai, bankininkystės sąsaja turi būti laikoma NDTS. Todėl ji turi būti įtraukta į kibernetinio saugumo rizikos vertinimą ir į esminių reikalavimų vykdymą viso produkto su skaitmeniniais elementais atžvilgiu. Tolesnis jau pateikto nurodymo tvarkymas, visų pirma operacijos registravimas sąskaitų valdymo ir apskaitos registro sistemose, atsiskaitymas ir tarpuskaita, atliekamas sistemose, su kuriomis programėlė tiesiogiai nesąveikauja, taigi vien dėl šios priežasties toks tvarkymas nėra NDTS.

— Sąskaitų valdymo sistema ir apskaitos registro sistema mobiliosios bankininkystės programėlės atžvilgiu nelaikomos NDTS. Programėlė su jomis tiesiogiai nesąveikauja (ji sąveikauja su bankininkystės sąsaja, kuri naudojasi šiomis sistemomis). Nors jų prieinamumas gali būti būtinas tam tikrai funkcijai visiškai atlikti, KAA apima tik tas sistemos dalis, kurios tiesiogiai sąveikauja su produktu su skaitmeniniais elementais. Todėl KAA taikymo tikslais šios sistemos nepatenka į NDTS apibrėžtį. Vis dėlto šios sistemos tebėra priklausomos nuo išorės veiksnių, dėl kurių produktui su skaitmeniniais elementais gali kilti reikšminga kibernetinio saugumo rizika. Pavyzdžiui, pažeidęs apskaitos registro sistemą, užpuolikas galėtų paveikti operacijų rezultatus, kurie vėliau rodomi programėlėje. Todėl gamintojas privalo nustatyti ir įvertinti tokią riziką atlikdamas kibernetinio saugumo rizikos vertinimą ir ją mažinti taikydamas priemones produkto lygmeniu, pavyzdžiui, užtikrindamas patikimą galinių sąsajų tapatumo nustatymą, operacijų duomenų vientisumo apsaugą, saugaus ryšio kanalus ir programėlės gaunamų atsakymų tikrinimą.

10 pav

Stilizuota NDTS grindžiamos bankininkystės programėlės schema



Trečiosios šalies SaaS klientų aptarnavimui:

— Finansų sektoriaus subjektas į savo programėlę integruoja klientų aptarnavimo pokalbių sprendinį, kurį sukūrė ir eksploatuoja paslaugas teikianti trečioji šalis; paslaugas teikianti trečioji šalis sukūrė pokalbių serverio kodą bei naudotojo sąsają ir eksploatuoja infrastruktūrą, kurioje įdiegtas pokalbių sprendinys (t. y. SaaS modelis).

— Kai klientas kreipiasi pagalbos, programėlė jį prijungia prie trečiosios šalies paslaugos, kad būtų pradėtas pokalbių seansas ir valdomas keitimasis pranešimais, nesuteikiant trečiajai šaliai prieigos prie pagrindinių banko sistemų.

Poveikis vertinant NDTS:

— Klientų aptarnavimo pokalbių sprendinys yra reikalingas tam, kad produktas su skaitmeniniais elementais galėtų atlikti vieną iš savo funkcijų, tačiau finansų sektoriaus subjektas jo neprojektavo ir nekūrė ir tai nebuvo daroma jo atsakomybe; todėl šis sprendinys nėra NDTS. Vis dėlto jis turėtų būti vertinamas kaip trečiosios šalies komponentas. Priklausomybė nuo šios trečiosios šalies paslaugos gali kelti kibernetinio saugumo riziką bankininkystės programėlei, pavyzdžiui, jei užpuolikas pasinaudotų pokalbių kanalu, kad apsimestų banko darbuotoju arba pateiktų naudotojams piktavališką turinį. Finansų sektoriaus subjektas turi atsižvelgti į šią riziką atlikdamas kibernetinio saugumo rizikos vertinimą ir ją mažinti taikydamas priemones produkto lygmeniu, pavyzdžiui, atskirdamas pokalbių funkciją nuo pagrindinių bankininkystės funkcijų, kontroliuodamas duomenų srautus ir tikrindamas turinį. Taip pat turėtų būti atliekamas SaaS sprendinio išsamus patikrinimas.

8.3.2. *Išmanusis termostatas*

Išmanusis termostatas suteikia naudotojams galimybę mobiliąja programėle valdyti temperatūrą savo namuose. Kad mobilioji programėlė ir išmanusis termostatas galėtų keistis duomenimis (pvz., perduoda prašymą padidinti temperatūrą) ir saugoti duomenis (pvz., naudotojo parinktis), tuos duomenis reikia tvarkyti nuotoliniu būdu. Šios funkcijos buvo suprojektuotos ir sukurtos gamintojo atsakomybe, tačiau jos veikia naudojant trečiosios šalies teikiamą pagrindinę fizinę ir virtualią infrastruktūrą (trečiosios šalies IaaS).

Nesant šio nuotolinio duomenų tvarkymo išmanusis termostatas negalėtų atlikti savo išmaniųjų funkcijų, vadinasi, produktas su skaitmeniniais elementais negalėtų atlikti vienos ar kelių savo funkcijų. Be to, programinė įranga buvo suprojektuota ir sukurta išmaniojo termostato gamintojo atsakomybe. Todėl nuotolinis duomenų tvarkymas laikomas NDTS, kaip apibrėžta KAA.

Atitikties KAA užtikrinimo tikslais išmaniojo termostato gamintojas produkto su skaitmeniniais elementais techniniuose dokumentuose turi aprašyti NDTS ir priklausomybę nuo trečiosios šalies IaaS, įskaitant informaciją apie sutartimi užsakytą paslaugą. Gamintojas turi atsižvelgti į šiuos elementus atlikdamas rizikos vertinimą, kuris apima produkto su skaitmeniniais elementais numatytąją paskirtį ir pagrįstai numatomą naudojimą. Atsižvelgdamas į su NDTS susijusią riziką, gamintojas įgyvendina KAA esminius reikalavimus. Trečiosios šalies IaaS atveju gamintojas turi užtikrinti, kad paslaugas teikiančios trečiosios šalies taikomos saugumo priemonės būtų tinkamos, ir (arba) imtis atitinkamų su infrastruktūra susijusių priemonių. Siekdamas įsitikinti, kad paslaugų teikėjo taikomos saugumo priemonės yra tinkamos, gamintojas galėtų, pavyzdžiui, paprašyti įrodymų, kad įvykdytos TIS 2 direktyvoje nustatytos pareigos.

8.3.3. *Elektroninių knygų skaityklė*

Elektroninių knygų skaityklės programinės įrangos gamintojas naudoja trečiosios šalies SaaS saugyklos paslaugą klientų įsigytoms elektroninėms knygoms saugoti ir jų prieigai prie įsigytų knygų suteikti. Nesant šios saugojimo paslaugos, produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų, tačiau trečiosios šalies SaaS saugojimo paslauga nėra sukurta gamintojo arba jo atsakomybe; SaaS teikėjas ją siūlo klientams bet kokiam naudojimo atvejui.

SaaS saugojimo paslauga neatitinka NDTS apibrėžties. Vis dėlto elektroninių knygų skaityklės gamintojas savo produkto su skaitmeniniais elementais veikimo tikslais naudojasi šia išorės paslauga, todėl turi atsižvelgti į susijusią riziką atlikdamas kibernetinio saugumo rizikos vertinimą. Elektroninių knygų skaityklės gamintojas turėtų SaaS paslaugą vertinti kaip komponentą. Gamintojas turi produkto lygmeniu įgyvendinti tinkamas saugumo priemones, pavyzdžiui, saugų tapatumo nustatymą, ryšio su saugojimo paslauga šifravimą ir vientisumo apsaugą. Išsamus patikrinimas parenkant ir integruojant SaaS teikėją taip pat padės gamintojui vykdyti savo pareigas, kad visas produktas su skaitmeniniais elementais galėtų atitikti esminius reikalavimus.

8.3.4. *Pramoninis robotas*

Pramoninio roboto užduotis – paimti detales. Robotas perduoda kameromis surinktą informaciją nuotolinei paslaugai, kurią suprojektavo ir sukūrė gamintojas. Ši paslauga veikia naudojant paslaugas teikiančios trečiosios šalies suteikiamą pagrindinę fizinę ir virtualią infrastruktūrą (trečiosios šalies IaaS). Debesijos paslauga pagal kamerų perduodamus duomenis apskaičiuoja detalės padėtį ir siunčia robotui komandas ją paimti.

Nesant tokio duomenų tvarkymo, pramoninis robotas negalėtų paimti detalių, taigi negalėtų atlikti vienos iš savo funkcijų. Be to, infrastruktūroje veikianti programinė įranga buvo suprojektuota ir sukurta gamintojo. Todėl gamintojo suprojektuota ir sukurta programinė įranga atitinka NDTS apibrėžtį.

Pramoninio roboto gamintojas produkto su skaitmeniniais elementais techniniuose dokumentuose turi aprašyti NDTS ir priklausomybę nuo trečiosios šalies IaaS, įskaitant informaciją apie sutartimi užsakytą paslaugą. Gamintojas taip pat turi atsižvelgti į šiuos elementus atlikdamas rizikos vertinimą, kuris apima produkto su skaitmeniniais elementais numatytąją paskirtį ir pagrįstai numatomą naudojimą. Atsižvelgdamas į riziką, gamintojas įgyvendina KAA esminius reikalavimus produkto su skaitmeniniais elementais, įskaitant jo NDTS, atžvilgiu. Išsamus patikrinimas pasirenkant IaaS teikėją taip pat padės gamintojui vykdyti savo pareigas. Pavyzdžiui, gamintojas galėtų paprašyti įrodymų, kad įvykdytos TIS 2 direktyvoje nustatytos pareigos.

8.3.5. *Korinio ryšio tinklas*

Išmaniajame telefone interneto ryšys, telefono skambučių ir žinučių siuntimo paslaugos (mobilusis ryšys) naudotojams teikiami naudojantis 5G tinklu. Korinio ryšio tinklą projektuoja ir kuria telekomunikacijų operatoriai. Tinklą sudaro mažosios bazinės stotys, mobiliojo ryšio bokštai ir kita tinklo įranga.

Produktas su skaitmeniniais elementais turi gebėti tinkamai prisijungti prie tinklo; tai yra viena iš jo funkcijų. Tačiau sprendžiant, ar produktas su skaitmeniniais elementais veikia tinkamai, nėra svarbu, ar pats tinklas tuo metu veikia. Tinklas yra tik ryšio kanalas ir nėra būtinas tam, kad produktas su skaitmeniniais elementais galėtų atlikti savo funkciją – tinkamai prisijungti prie tinklo. Analogiškai eterneto kabelis, maršruto parinktuvas ar Wi-Fi signalas nelaikomi duomenų tvarkymu, kurio nesant produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų; jie veikiau sudaro sąlygas ryšiui ir (arba) junglumui.

Todėl korinio ryšio tinklas neatitinka NDTS apibrėžties. Tinklas taip pat neturėtų būti vertinamas kaip trečiosios šalies komponentas, nes į produktą su skaitmeniniais elementais nėra integruojama jokia su šiuo tinklu susijusi programinė įranga – produktas tik naudojasi šiuo tinklu. Todėl gamintojui nebūtina tinklo paslaugų teikėjo atžvilgiu atlikti išsamaus patikrinimo pareigų.

9. **PAPILDOMI ELEMENTAI**

9.1. **Pareigos pranešti**

209. Pagal KAA 14 straipsnio 1 ir 3 dalis gamintojas privalo vienu metu pranešti koordinatoriumi paskirtai CSIRT ir ENISA apie: i) bet kokį aktyviai išnaudojamą jo produkto su skaitmeniniais elementais pažeidžiamumą, apie kurį jis sužino, ir ii) bet kokį didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, apie kurį jis sužino.

210. Pagal 69 straipsnio 3 dalį ir 71 straipsnio 2 dalies antrą sakinį pareiga laikytis 14 straipsnio nuo 2026 m. rugsėjo 11 d. taikoma visiems į KAA taikymo sritį patenkantiems produktams su skaitmeniniais elementais, įskaitant produktus su skaitmeniniais elementais, pateiktus rinkai anksčiau nei 2027 m. gruodžio 11 d. Be to, skirtingai nuo pažeidžiamumo valdymo pareigų, kurios taikomos tik produkto palaikymo laikotarpiu, pareigos pranešti tebetaikomos ir pasibaigus produkto su skaitmeniniais elementais palaikymui. Jei produktas su skaitmeniniais elementais buvo pateiktas rinkai anksčiau nei 2027 m. gruodžio 11 d. arba jei pasibaigė jo palaikymo laikotarpis, gamintojas neprivalo atlikti I priedo II dalyje nustatytų pažeidžiamumo valdymo pareigų.

211. Reikėtų priminti, kad pareiga pranešti apie tokius įvykius taikoma nuo tada, kai gamintojas sužino, kad pažeidžiamumas yra aktyviai išnaudojamas arba kad įvyko didelis incidentas, dėl kurio kilo pavojus jo produkto su skaitmeniniais elementais saugumui. Todėl gairės dėl to, kada laikoma, kad gamintojas apie tai sužinojo, turėtų padėti gamintojams nustatyti momentą, nuo kurio pradedami skaičiuoti taikomi pranešimo terminai.

212. Gamintojams pagal skirtingus ES teisės aktus gali būti taikomos panašios pareigos pranešti. Siekiant užtikrinti, kad sąvoka „sužinojimas“ būtų aiškinama nuosekliai, ir palengvinti gamintojams šių pareigų vykdymą, šios gairės suderintos su Komisijos įgyvendinimo reglamento (ES) 2024/2690 31 konstatuojamąja dalimi ir Gairių 9/2022 dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR II skyriaus A skirsniu.

213. Kai kuriais atvejais gamintojas pats aptiks įtartiną įvykį arba trečioji šalis, pavyzdžiui, fizinis asmuo, klientas, subjektas, institucija, žiniasklaidos organizacija ar kitas šaltinis, atkreips jo dėmesį į galimą incidentą ar pažeidžiamumą. Tokiais atvejais gamintojas įtartiną įvykį turėtų įvertinti nedelsdamas, kad nustatytų, ar tai yra aktyviai išnaudojamas pažeidžiamumas, ar didelis incidentas, darantis poveikį produkto su skaitmeniniais elementais saugumui. Todėl laikoma, kad gamintojas apie tai sužinojo, kai, atlikęs tokį pirminį vertinimą, jis yra pagrįstai įsitikinęs, kad i) jo produkto su skaitmeniniais elementais pažeidžiamumas yra aktyviai išnaudojamas arba ii) įvyko didelis incidentas, dėl kurio kilo pavojus jo produkto su skaitmeniniais elementais saugumui.

214. Taigi momentas, nuo kurio gamintojas gali būti laikomas sužinojusiu apie tokį įvykį, priklausys nuo konkretaus aktyviai išnaudojamo pažeidžiamumo ar didelio incidento aplinkybių. Kai kuriais atvejais nuo pat pradžių bus gana aišku, kad pažeidžiamumas yra aktyviai išnaudojamas arba kad didelis incidentas daro poveikį produkto su skaitmeniniais elementais saugumui. Kitais atvejais gali prireikti šiek tiek laiko nustatyti, ar produktas su skaitmeniniais elementais yra pažeidžiamas ir ar tą pažeidžiamumą išnaudoja piktavalis subjektas arba ar incidentas daro poveikį produkto su skaitmeniniais elementais saugumui. Vis dėlto svarbiausia yra nedelsiant imtis veiksmų ir atlikti pirminį vertinimą, siekiant nustatyti, ar šios sąlygos iš tiesų yra tenkinamos, ypač kai pažeidžiamumas gali kelti didelę riziką, o jei jos tenkinamos – imtis taisomųjų veiksmų ir pateikti pranešimą pagal KAA.

215. Be to, pareigų pranešti struktūra yra tokia, kad gamintojai turi laipsniškai atnaujinti savo pranešimus, kai jų vidaus tyrimai pasiekia tolesnius etapus ir gaunama išsamesnės informacijos apie aktyviai išnaudojamą pažeidžiamumą ar incidentą. Visų pirma gamintojai privalo nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas nuo tada, kai apie tai sužino, pateikti ankstyvąjį perspėjimą, kuriame pateikiama ribotos apimties informacija. Vėliau papildoma informacija turi būti pateikta pranešime, kuris pateikiamas nepagrįstai nedelsiant ir bet kuriuo atveju per 72 valandas nuo tada, kai apie tai sužinoma, (toliau – per 72 valandas pateiktinas pranešimas). Išsamus pranešimas apie aktyviai išnaudojamą pažeidžiamumą turi būti pateiktas per 14 dienų nuo tada, kai tampa prieinama taisomoji ar rizikos mažinimo priemonė, o apie didelius incidentus – per vieną mėnesį nuo per 72 valandas pateiktino pranešimo pateikimo.

216. Kaip taip pat primenama *3.3.1* skirsnyje „*Nuolatinė parama ir FOSS gyvybingumo užtikrinimas*“, atvirosios programinės įrangos valdytojai pagal 24 straipsnio 3 dalį taip pat privalo pranešti apie aktyviai išnaudojamą pažeidžiamumą ([30]). Ši pareiga nėra taikoma vien dėl to, kad FOSS, kurios valdytojas yra tas subjektas, programinio kodo bazėje yra pažeidžiamumas, ji taikoma tada, kai sužinoma, kad pažeidžiamumas yra aktyviai išnaudojamas. Praktiškai, kadangi FOSS komponentai paprastai integruojami į kitus tolesnius produktus su skaitmeniniais elementais, tikėtina, kad apie aktyvų išnaudojimą valdytojas sužinos iš trečiųjų šalių pranešimų, kuriuose nustatoma, kad FOSS komponentai, integruoti į kitus produktus su skaitmeniniais elementais, yra aktyviai išnaudojami. Taip gali būti, pavyzdžiui, kai produkto su skaitmeniniais elementais gamintojas aptinka aktyvų į jo paties produktą integruoto FOSS komponento išnaudojimą ir apie tai praneša to komponento valdytojui arba kai naudotojas ar saugumo tyrėjas aptinka į produktą su skaitmeniniais elementais integruoto FOSS komponento išnaudojimo požymių ir apie tokį aktyvų išnaudojimą praneša komponento valdytojui.

217. Taip pat reikėtų paaiškinti, kad, nors pareiga pranešti apie aktyviai išnaudojamą pažeidžiamumą taikoma nuo tada, kai gamintojas sužino apie aktyvų išnaudojimą, gamintojas neprivalo pranešti apie pažeidžiamumą, apie kurio aktyvų išnaudojimą jis jau buvo sužinojęs iki 2026 m. rugsėjo 11 d. (datos, nuo kurios pradedama taikyti pareiga pranešti). Taigi KAA nereikalaujama apie tokį pažeidžiamumą pranešti atgaline data. Kita vertus, pareiga pranešti taikoma tais atvejais, kai gamintojas apie pažeidžiamumą žinojo iki 2026 m. rugsėjo 11 d., tačiau tuo metu nežinojo apie jokį aktyvų jo išnaudojimą (nes toks išnaudojimas dar nebuvo prasidėjęs arba gamintojas apie jį dar nebuvo sužinojęs). Jei po 2026 m. rugsėjo 11 d. pažeidžiamumas pradedamas aktyviai išnaudoti arba gamintojas sužino apie tokį išnaudojimą, laikoma, kad tai yra aktyviai išnaudojamas pažeidžiamumas, dėl kurio taikoma pareiga pranešti.

218. Gamintojas taip pat privalo pranešti tik apie aktyviai išnaudojamą jo produkto su skaitmeniniais elementais pažeidžiamumą. Jei produkto su skaitmeniniais elementais pažeidžiamumas yra aktyviai išnaudojamas dėl trečiosios šalies komponento, produkto su skaitmeniniais elementais gamintojas privalo pranešti apie tą aktyviai išnaudojamą pažeidžiamumą. Tačiau jei gamintojas žino apie trečiosios šalies komponento pažeidžiamumą, bet tas pažeidžiamumas arba i) negali būti išnaudojamas jo produkte su skaitmeniniais elementais (pavyzdžiui, dėl to, kad pažeidžiamas kodas nėra pasiekiamas), arba ii) nebuvo išnaudotas jo produkte su skaitmeniniais elementais, toks pažeidžiamumas nelaikomas aktyviai išnaudojamu jo produkto su skaitmeniniais elementais pažeidžiamumu, todėl tam gamintojui apie jį pranešti neprivaloma. Vis dėlto tas gamintojas gali apie tokį pažeidžiamumą pranešti savanoriškai pagal KAA 15 straipsnį. Jis taip pat privalo laikytis KAA I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų ir pranešti apie pažeidžiamumą komponentą gaminančiam ar techniškai prižiūrinčiam asmeniui arba subjektui pagal 13 straipsnio 6 dalį, kaip išsamiau paaiškinta *9.2.1* skirsnyje „*Pranešimų teikimas pirmesnės tiekimo grandies subjektams* ir dalijimasis saugumo pataisomis“.

([30]) Jei valdytojas dalyvauja kuriant produktą su skaitmeniniais elementais.

219. Sužinoję apie aktyviai išnaudojamą pažeidžiamumą arba didelį incidentą, gamintojai pagal 14 straipsnio 8 dalį taip pat privalo informuoti paveiktus naudotojus ir, kai tinkama, visus kitus naudotojus. Jeigu jie to laiku nepadaro, pranešimą gavusios CSIRT gali pateikti tokią informaciją naudotojams, kai manoma, kad tai proporcinga ir būtina siekiant užkirsti kelią to pažeidžiamumo ar incidento poveikiui arba jį sumažinti.

220. Laikantis rizika grindžiamo požiūrio pagal KAA, 14 straipsnio 8 dalyje nustatyta pareiga informuoti naudotojus turi būti taikoma atsižvelgiant į riziką ir proporcingai. Visų pirma informacijos apie aktyviai išnaudojamą pažeidžiamumą ar didelį incidentą pateikimas nereiškia, kad tokia informacija turi būti viešai paskelbta arba atskleista neapibrėžtam gavėjų ratui. Kai tinkama ir atsižvelgdami į produkto su skaitmeniniais elementais pobūdį, paveiktus naudotojus ir galimą pažeidžiamumo ar incidento poveikį, gamintojai gali išsamią informaciją atskleisti tik atitinkamiems paveiktiems naudotojams ar klientams. Tai ypač aktualu produktų su skaitmeniniais elementais, naudojamų jautrioje ar esminės svarbos aplinkoje, atveju, kai viešas techninės informacijos atskleidimas pats savaime galėtų padidinti kibernetinio saugumo riziką arba sudaryti palankesnes sąlygas tolesniam išnaudojimui.

221. Kai pažeidžiamumas tinkamai pašalinamas arba jo poveikis sumažinamas, gali būti tikslinga informaciją atskleisti plačiau. Taip būtų, pavyzdžiui, tais atvejais, kai informacijos atskleidimas padeda didinti bendrą informuotumą arba suteikia naudotojams galimybę patikrinti, ar jų produktams su skaitmeniniais elementais pažeidžiamumas nebedaro poveikio. Tokiais atvejais platesnio informacijos atskleidimo išsamumo lygis ir laikas turėtų išlikti proporcingi, atsižvelgiant į liekamąją pažeidžiamumo išnaudojimo riziką, produkto su skaitmeniniais elementais pobūdį ir atitinkamų naudotojų interesus. Be to, I priedo II dalies 4 punkte reikalaujama, kad, kai tik tampa prieinamas saugumo naujinys, gamintojai viešai atskleistų informaciją apie pašalintus pažeidžiamumus.

9.2. **Pažeidžiamumo valdymas**

9.2.1. *Pranešimų teikimas pirmesnės tiekimo grandies subjektams ir dalijimasis saugumo pataisomis*

222. KAA 13 straipsnio 6 dalyje reikalaujama, kad gamintojai apie integruotuose komponentuose nustatytą pažeidžiamumą praneštų tą komponentą gaminančiam ar techniškai prižiūrinčiam asmeniui arba subjektui (pranešimas pirmesnės tiekimo grandies subjektams).

223. Gamintojai tokius pranešimus privalo teikti tik dėl tos komponento versijos, kurią jie yra integravę. Jeigu komponentą gaminantis ar techniškai prižiūrintis asmuo arba subjektas yra nustatęs saugumo politiką, koordinuoto pažeidžiamumo atskleidimo procesus ar specialius pranešimo apie pažeidžiamumą kanalus, gamintojai turėtų pranešti laikydamiesi tokių taisyklių ir procesų, ypač tais atvejais, kai per ankstyvas informacijos apie dar neištaisytą pažeidžiamumą atskleidimas galėtų padidinti kibernetinio saugumo riziką. Be to, siekiant sumažinti pirmesnės tiekimo grandies techninės priežiūros vykdytojams tenkančią naštą, ypač atvirojo kodo projektuose, gamintojai tokio pranešimo pirmesnės tiekimo grandies subjektams teikti neprivalo, jeigu gali patvirtinti, kad komponentą gaminantis ar techniškai prižiūrintis asmuo arba subjektas apie pažeidžiamumą jau žino. Gamintojai raginami imtis pagrįstų priemonių, kad būtų išvengta pasikartojančių pranešimų teikimo, pavyzdžiui, prieš teikiant pranešimą pirmesnės tiekimo grandies subjektams patikrinti viešai prieinamas pažeidžiamumo duomenų bazes, konkretaus projekto saugumo pranešimus arba naudojamas problemų fiksavimo sistemas.

224. Gamintojai privalo teikti pranešimus pirmesnės tiekimo grandies subjektams tik apie paties integruoto komponento pažeidžiamumą, o ne apie pažeidžiamumą, atsiradusį dėl to komponento integravimo su kitu gamintojo sukurtu programiniu kodu arba dėl kitų komponentų integravimo. Vis dėlto gali pasitaikyti atvejų, kai komponentą integravus į konkretų produktą su skaitmeniniais elementais išryškėja tam tikra to komponento elgsena, sąveika ar saugumui svarbios savybės, kurios vertinant komponentą atskirai nebuvo akivaizdžios arba lengvai nustatomos. Tokiais atvejais gamintojai raginami šią informaciją perduoti komponentą gaminančiam ar techniškai prižiūrinčiam asmeniui arba subjektui, taip skatinant gerąją pažeidžiamumo valdymo praktiką, kuria siekiama sudaryti sąlygas veiksmingai pašalinti pažeidžiamumą ir didinti bendrą komponentų ekosistemos saugumą.

225. Galiausiai, gamintojai taip pat neprivalo pranešti apie pažeidžiamumą pirmesnės tiekimo grandies subjektams, jeigu komponento nebeprižiūri joks techninės priežiūros vykdytojas arba jeigu gamintojas naujų versijų ar saugumo pataisų atžvilgiu nebesikliauja pirminio techninės priežiūros vykdytojo atliekama priežiūra. Vis dėlto tokiais atvejais gamintojas raginamas apie pažeidžiamumą informuoti to komponento naudotojus kitomis pagrįstomis priemonėmis, pavyzdžiui, pasitelkdamas esamus bendruomenės mechanizmus (tokius kaip elektroninio pašto adresatų sąrašai ar problemų registravimo įrašai) arba viešus pažeidžiamumo registrus.

226. Be to, pagal 13 straipsnio 6 dalį gamintojai, kurie sukūrė integruoto komponento pažeidžiamumui pašalinti skirtą programinės įrangos pakeitimą (saugumo pataisą), privalo tuo programinės įrangos pakeitimu pasidalyti su komponentą gaminančiu ar techniškai prižiūrinčiu asmeniu arba subjektu (dalijimasis su pirmesnės tiekimo grandies subjektu).

227. Kai pagal 13 straipsnio 6 dalį gamintojai privalo pasidalyti saugumo pataisa, ši pataisa, kai tinkama, turėtų būti pateikta kompiuterio skaitomu formatu ir tokiu būdu, kad komponentą gaminantis ar techniškai prižiūrintis asmuo arba subjektas galėtų ją lengvai patikrinti ir, kai tinkama, integruoti. Jei komponentas yra laisvosios ir atvirosios programinės įrangos komponentas, saugumo pataisa turėtų būti perduodama tokiu būdu, kuris būtų suderinamas su to komponento licencija, pavyzdžiui, ja dalijantis pagal tą pačią licenciją arba pagal licenciją, leidžiančią techninės priežiūros vykdytojui platinti pataisą pagal savo licenciją. Jei to komponento techninės priežiūros vykdytojas yra nustatęs gaires, kaip turėtų būti dalijamasi saugumo pataisomis, gamintojas turėtų jų laikytis.

228. Tačiau pagal KAA gamintojai neprivalo užtikrinti, kad komponentą gaminantis ar techniškai prižiūrintis asmuo arba subjektas jų saugumo pataisas būtinai priimtų. Jie taip pat neprivalo užtikrinti, kad tos pataisos būtinai būtų integruotos į komponento programinio kodo saugyklą, pavyzdžiui, kai techninės priežiūros vykdytojas gali teikti pirmenybę kitokiam problemos sprendimo būdui. Gamintojai taip pat neprivalo priimti komponento techninės priežiūros vykdytojo pasiūlytos pataisos ir gali pasirinkti problemos keliamą riziką sumažinti kitais tinkamais būdais.

229. Kai kuriais atvejais komponentą gaminantis ar techniškai prižiūrintis asmuo arba subjektas jau gali būti pateikęs saugumo pataisą pažeidžiamumui pašalinti, tačiau gamintojas gali taikyti kitokią rizikos mažinimo strategiją (pavyzdžiui, pakeisti konfigūraciją kita). Tokiais atvejais pagal KAA nereikalaujama, kad gamintojas su pirmesnės tiekimo grandies subjektu dalytųsi kitos sistemos dalies pakeitimu. Vis dėlto gamintojas raginamas tai daryti, kai tai gali būti naudinga komponentą techniškai prižiūrinčiam asmeniui arba subjektui.

9.2.2. *Žinomas pažeidžiamumas, kuris gali būti išnaudojamas*

230. Viename iš KAA I priedo I dalyje išdėstytų esminių reikalavimų nustatyta, kad, remiantis 13 straipsnio 2 dalyje nurodytu kibernetinio saugumo rizikos vertinimu ir kai taikytina, produktai su skaitmeniniais elementais turi būti tiekiami rinkai be jokio žinomo pažeidžiamumo, kurį būtų galima išnaudoti.

231. 3 straipsnio 41 punkte „pažeidžiamumas, kurį galima išnaudoti“ apibrėžiamas kaip „pažeidžiamumas, kurį gali veiksmingai panaudoti priešininkas praktinėmis veiklos sąlygomis“. Ne visus pažeidžiamumus galima išnaudoti praktinėmis veiklos sąlygomis, o kai kuriuos pažeidžiamumus galima išnaudoti tik teorinėmis sąlygomis (pavyzdžiui, laboratorijoje ar atliekant modeliavimą) ir (arba) tokiomis sąlygomis, kurių produkto su skaitmeniniais elementais veikimo aplinkoje nebūtų.

232. KAA reikalaujama, kad gamintojai turėtų tinkamą politiką ir procedūras galimam pažeidžiamumui, apie kurį pranešė vidaus ar išorės šaltiniai, valdyti ir pašalinti (13 straipsnio 8 dalis). Tačiau KAA aiškiai nenurodyta, nuo kada turi būti laikoma, kad gamintojas žino apie pažeidžiamumą, kurį galima išnaudoti, ir dėl to produkto pateikimo rinkai momentu atsiranda pareiga laikytis šio esminio reikalavimo.

233. Pažeidžiamumas turėtų būti laikomas žinomu, kai jis įtrauktas į atitinkamas viešai prieinamas pažeidžiamumo duomenų bazes, pavyzdžiui, Europos pažeidžiamumų duomenų bazę, sukurtą pagal Direktyvos (ES) 2022/2555 12 straipsnio 2 dalį, arba kitas plačiai naudojamas pažeidžiamumo duomenų bazes.

234. Be to, pažeidžiamumas taip pat gali būti laikomas žinomu, kai gamintojas apie jį sužino iš neviešos informacijos, pavyzdžiui, saugumo tyrėjui koordinuotai atskleidus pažeidžiamumą arba gamintojui pačiam atliekant vidaus bandymus ir analizę, įskaitant, pavyzdžiui, naudojimąsi DI grindžiamomis paslaugomis. Pažeidžiamumas taip pat gali būti laikomas žinomu, kai apie jį viešai ir plačiai pranešama patikimomis žiniasklaidos priemonėmis, įskaitant specializuotus kibernetinio saugumo leidinius ar bendrąją žiniasklaidą.

235. Vis dėlto vien tai, kad apie pažeidžiamumą pranešta arba kad jis aptiktas, savaime nereiškia, kad jį galima išnaudoti praktiškai arba kad jis yra aktualus atitinkamam konkrečiam produktui su skaitmeniniais elementais. Gamintojas turės jį ištirti ir patvirtinti tokios informacijos tikrumą bei jos aktualumą savo produktui su skaitmeniniais elementais. Todėl nuo pirmojo pranešimo apie pažeidžiamumą iki jo patvirtinimo gali praeiti tam tikras ribotas laikas. Kaip nurodyta *9.1* skirsnyje *„Pareigos pranešti“*, svarbiausia yra nedelsiant imtis veiksmų pažeidžiamumui ištirti ir į jį reaguoti.

236. Be to, pagal 13 straipsnio 1 dalį gamintojų pareiga laikytis I priedo I dalyje nustatytų esminių reikalavimų taikoma produkto pateikimo rinkai momentu. Praktiškai gali pasitaikyti atvejų, kai naujas pažeidžiamumas, kurį potencialiai galima išnaudoti, aptinkamas galutiniuose produkto su skaitmeniniais elementais kūrimo ciklo etapuose, įskaitant laikotarpį prieš pat jam patenkant į platinimo grandinę (taigi prieš pat jo pateikimą rinkai).

237. Kadangi pareiga produktus su skaitmeniniais elementais pateikti rinkai be jokio žinomo pažeidžiamumo, kurį būtų galima išnaudoti, yra rizika grindžiama pareiga, gamintojas, remdamasis kibernetinio saugumo rizikos vertinimu, turi nustatyti, ar produktas su skaitmeniniais elementais gali būti saugiai pateiktas rinkai laikantis KAA. Arba gamintojas gali nuspręsti, kad naujai paaiškėjęs pažeidžiamumas turi būti pašalintas prieš pateikiant produktą su skaitmeniniais elementais rinkai. Priimdami tokį sprendimą gamintojai turėtų atsižvelgti į pažeidžiamumo sunkumą, galimybę jį išnaudoti ir galimą jo poveikį, taip pat į riziką, kuri, pradėjus produktą su skaitmeniniais elementais naudoti, kyla pačiam produktui. Jie taip pat gali atsižvelgti į riziką, kuri kiltų atidėjus produkto išleidimą iki pažeidžiamumo pašalinimo, pavyzdžiui, kai naujoje versijoje taip pat pašalinamas kitas pažeidžiamumas, kurį galima išnaudoti, arba kai nauja versija yra būtina nenutrūkstamam ypatingos svarbos sistemų veikimui užtikrinti. Bet kuriuo atveju, pateikus produktą su skaitmeniniais elementais rinkai, gamintojui ir toliau taikoma pareiga veiksmingai valdyti pažeidžiamumą laikantis I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų.

9.2.3. *Veiksmingi ir reguliarūs bandymai ir peržiūros*

238. I priedo II dalies 3 punkte reikalaujama, kad gamintojai per visą produkto su skaitmeniniais elementais palaikymo laikotarpį atliktų veiksmingus ir reguliarius to produkto bandymus ir peržiūras. Reguliarus bandymų atlikimas nereiškia, kad ta pati nepakeista bandymų serija turi būti mechaniškai kartojama nustatytais intervalais. Tai reiškia, kad turi būti reguliariai vertinama, ar dėl naujų duomenų, pavyzdžiui, naujai nustatytų grėsmių ar naujai aptikto pažeidžiamumo, reikia atnaujinti esamus bandymus, ir atitinkamai atliekami bandymai.

239. Peržiūrų dažnumas, išsamumas ir turinys turėtų būti proporcingi produkto su skaitmeniniais elementais kibernetinio saugumo rizikos profiliui, jo kitimui laikui bėgant ir esamai grėsmių aplinkai. Jeigu atliekant peržiūrą nustatoma naujų reikšmingų duomenų, turinčių įtakos bandymų rinkiniui, turėtų būti parengti ir atlikti nauji arba pakeisti produkto bandymai, siekiant užtikrinti, kad neliktų nepašalinto pažeidžiamumo. Tai gali apimti ir pakartotinį esamų bandymų atlikimą, kai dėl produkto su skaitmeniniais elementais pakeitimo tokio pobūdžio bandymai tampa tikslingi, pavyzdžiui, regresinį testavimą.

240. Jeigu atliekant peržiūrą tokių duomenų nenustatoma, papildomų bandymų numatyti nereikia. Kitos pažeidžiamumo valdymo pareigos, įskaitant pareigą šalinti pažeidžiamumą ir imtis taisomųjų priemonių atsižvelgiant į pažeidžiamumo keliamą riziką, ir toliau taikomos lygiagrečiai.

9.3. **Sąveika su kitais teisės aktais**

9.3.1. *Reglamentas (ES) 2019/2144 ir Reglamentas (ES) Nr. 168/2013*

241. KAA 2 straipsnio 2 dalies c punkte nustatyta, kad reglamentas netaikomas produktams su skaitmeniniais elementais, kuriems taikomas Reglamentas (ES) 2019/2144. Reglamentas (ES) 2019/2144 taikomas „M, N ir O kategorijų transporto priemonėms, kaip apibrėžta Reglamento (ES) 2018/858 4 straipsnyje, taip pat joms skirtoms sistemoms, sudėtinėms dalims ir atskiriems techniniams mazgams“.

242. Panašiai produktai su skaitmeniniais elementais, patenkantys į Reglamento (ES) Nr. 168/2013 taikymo sritį, Komisijos deleguotuoju reglamentu (ES) 2025/1535 buvo pašalinti iš KAA taikymo srities. Reglamentas (ES) Nr. 168/2013 taikomas L kategorijos transporto priemonėms, „tokioms transporto priemonėms suprojektuotoms ir sukonstruotoms sistemoms, komponentams ir atskiriems techniniams mazgams“, taip pat dalims ir įrangai (2 straipsnio 1 dalis).

243. Transporto priemonėms, kurioms taikomi šie reglamentai, KAA netaikomas. Be to, reikia papildomai paaiškinti išimties taikymo sistemoms, komponentams, atskiriems techniniams mazgams, dalims ir įrangai (šiame skirsnyje toliau – komponentai), suprojektuotiems ir sukonstruotiems tokioms transporto priemonėms ir laikomiems produktais su skaitmeniniais elementais pagal KAA, aprėptį.

244. Laikoma, kad tokiems komponentams KAA netaikomas, jeigu jie suprojektuoti ir sukonstruoti tik tam, kad būtų integruoti į transporto priemones, kurioms taikomi reglamentai (ES) 2019/2144 ir (ES) Nr. 168/2013. Taip yra nepriklausomai nuo to, ar to komponento gamintojas jį parduoda tiesiogiai transporto priemonės gamintojui, ar kitam automobilių sektoriaus tiekimo grandinės ekonominės veiklos vykdytojui, jeigu komponentas yra aiškiai skirtas ir tinkamas tik galutiniam integravimui į tokias transporto priemones.

245. Kita vertus, gamintojui, parduodančiam bendrosios paskirties komponentus, kurie yra produktai su skaitmeniniais elementais ir kuriuos galima integruoti į įvairių rūšių produktus, o ne vien į transporto priemones, kurioms taikomi minėti reglamentai, KAA yra taikomas.

246. Vertinimas, ar komponentas pateikiamas rinkai, kaip tai suprantama pagal KAA, turi būti grindžiamas objektyviomis sąlygomis, kuriomis tas komponentas tiekiamas rinkai. Jei komponentą, kuris yra tinkamas ne tik galutiniam integravimui į tokias transporto priemones, gamintojas siūlo per platinimo kanalus, kuriais gali naudotis ir automobilių sektoriaus tiekimo grandinei nepriklausantys klientai, pavyzdžiui, per bendrosios mažmeninės prekybos vietas arba internetinės prekybos kanalus, priimančius užsakymus iš plačiosios visuomenės, toks komponentas patenka į KAA taikymo sritį, neatsižvelgiant į jokius pareiškimus dėl numatomos jo paskirties. Tokiomis aplinkybėmis komponentas negali būti laikomas suprojektuotu ir sukonstruotu vien integruoti į transporto priemones, kurioms taikomi reglamentai (ES) 2019/2144 ir Nr. 168/2013, todėl gamintojas privalo laikytis KAA. Kita vertus, ribotų įmonių tarpusavio (B2B) platinimo kanalų, skirtų tik automobilių sektoriaus tiekimo grandinei, naudojimas gali rodyti, kad komponentas yra suprojektuotas ir sukonstruotas vien tokiam integravimui.

9.3.2. *ES tipo tyrimo sertifikatų galiojimas (69 straipsnio 1 dalis)*

247. KAA 69 straipsnio 1 dalyje nustatyta, kad „ES tipo tyrimo sertifikatai ir patvirtinimo sprendimai dėl produktų su skaitmeniniais elementais, kuriems taikomi kiti nei šis reglamentas Sąjungos derinamieji teisės aktai, kibernetinio saugumo reikalavimų galioja iki 2028 m. birželio 11 d., išskyrus atvejus, kai jie nustoja galioti anksčiau nei tą datą arba kai tuose kituose Sąjungos derinamuosiuose teisės aktuose nurodyta kitaip – tokiu atveju jie galioja tiek, kiek nurodyta tuose teisės aktuose“.

248. Tolesnis tokių sertifikatų ir patvirtinimo sprendimų galiojimas turėtų būti suprantamas kaip apribotas kibernetinio saugumo rizika ir atitinkamais reikalavimais, kuriems taikomi atitinkami Sąjungos derinamieji teisės aktai, kuriais remiantis tie sertifikatai ar sprendimai buvo išduoti. Dėl tokios rizikos gamintojai neprivalo vien KAA taikymo tikslais iš naujo atlikti produktų su skaitmeniniais elementais, kuriuos jie ketina pateikti rinkai ne anksčiau kaip 2027 m. gruodžio 11 d. ir iki 2028 m. birželio 11 d., rizikos vertinimo ar iš naujo įrodyti jų atitikties per 69 straipsnio 1 dalyje nurodytą galiojimo laikotarpį ([31]). Tai taikoma tiek sertifikatams ir patvirtinimo sprendimams, išduotiems tais atvejais, kai pagal taikytinus Sąjungos derinamuosius teisės aktus gamintojas privalo atlikti atitikties vertinimo procedūrą pasitelkdamas notifikuotąją įstaigą, tiek tais atvejais, kai gamintojas tokią procedūrą pasirinko savo noru.

249. Todėl galiojantis sertifikatas arba patvirtinimo sprendimas, išduotas pagal kitus Sąjungos derinamuosius teisės aktus, neatleidžia gamintojų nuo pareigos pagal KAA atlikti išsamų kibernetinio saugumo rizikos vertinimą (ar nuo kitų KAA nustatytų pareigų). Tačiau atlikdami atitikties vertinimo procedūrą jie gali remtis jau turimais sertifikatais kaip atitikties įrodymu tiek, kiek atitinkama kibernetinio saugumo rizika jau yra įvertinta pagal tuos sertifikatus. Jei pagal kitus Sąjungos derinamuosius teisės aktus sertifikatas ar patvirtinimo sprendimas galioja ilgiau nei iki 2028 m. birželio 11 d., KAA taikymo tikslais gamintojas tokiu sertifikatu ar sprendimu vis vien gali remtis tik iki 2028 m. birželio 11 d.

250. Jei pagal 13 straipsnio 2 dalį atlikus kibernetinio saugumo rizikos vertinimą nustatoma papildoma rizika, kurios neapima kibernetinio saugumo reikalavimai, kuriais grindžiamas esamas sertifikatas ar patvirtinimo sprendimas, gamintojai ir toliau atsako už tos rizikos valdymą pagal KAA. Tokiais atvejais, siekiant užtikrinti atitiktį, nustatyti trūkumai turi būti įvertinti, o su jais susijusi rizika sumažinta, nepaisant to, kad esamas sertifikatas ar patvirtinimo sprendimas tebegalioja.

251. Tai galima iliustruoti atveju, kai produktui su skaitmeniniais elementais taikomi kibernetinio saugumo reikalavimai, nustatyti Komisijos deleguotajame reglamente (ES) 2022/30, kuriuo papildoma Direktyva 2014/53/ES, (Radijo įrenginių direktyvos (RĮD) deleguotajame akte) ir remiantis tais reikalavimais yra išduotas ES tipo tyrimo sertifikatas arba patvirtinimo sprendimas. Tokiu atveju pagal 69 straipsnio 1 dalį sertifikatas ar sprendimas ir toliau galioja tai kibernetinio saugumo rizikai, kurią jis apima ir kuri yra susijusi su Direktyvoje 2014/53/ES (Radijo įrenginių direktyvoje, RĮD) nustatytais esminiais kibernetinio saugumo reikalavimais.

252. Tokiais atvejais KAA taikymo tikslais gamintojai neprivalo iš naujo vertinti ar iš naujo įrodyti atitikties reikalavimams dėl tos rizikos, kuri jau buvo įvertinta išduodant tokius sertifikatus, tol, kol atitinkamas sertifikatas ar patvirtinimo sprendimas galioja, ir bet kuriuo atveju ne ilgiau kaip iki 2028 m. birželio 11 d. Tai apima, pavyzdžiui, su tinklo apsauga, asmens duomenų ir privatumo apsauga ar sukčiavimo prevencija susijusią kibernetinio saugumo riziką (tiek, kiek tokią riziką apima tas sertifikatas), kuri yra susijusi su RĮD kibernetinio saugumo reikalavimais ir į kurią atsižvelgta atliekant atitikties vertinimą.

253. Tačiau jei pagal KAA 13 straipsnio 2 dalį atlikus kibernetinio saugumo rizikos vertinimą nustatoma papildoma kibernetinio saugumo rizika, kurios tie sertifikatai neapima, gamintojai ir toliau atsako už tokios rizikos valdymą pagal KAA. Tai gali apimti, pavyzdžiui, riziką, susijusią su pažeidžiamumo valdymo procesais, duomenų kiekio ir atakos pažeidžiamos srities mažinimu, arba kitus konkrečiam produktui būdingus kibernetinio saugumo aspektus, kurių neapima tie sertifikatai arba kurių bet kuriuo atveju neapima RĮD nustatyti esminiai kibernetinio saugumo reikalavimai.

254. Todėl vien galiojančio ES tipo tyrimo sertifikato ar patvirtinimo sprendimo, išduoto pagal RĮD dėl jos esminių su kibernetiniu saugumu susijusių reikalavimų, buvimas savaime neįrodo visiškos atitikties KAA. Tačiau tai leidžia gamintojams remtis tokiu sertifikatu ar sprendimu kaip atitikties įrodymu dėl atitinkamos rizikos, kartu užtikrinant, kad visa likusi ar naujai nustatyta rizika būtų įvertinta ir sumažinta pagal KAA.

([31]) Produktams su skaitmeniniais elementais, pateiktiems rinkai anksčiau nei 2027 m. gruodžio 11 d., taikomi Sąjungos teisės aktai, taikytini jų pateikimo rinkai metu, ir, jei tie produktai juos atitinka, jie gali būti toliau parduodami ir pradedami eksploatuoti, išskyrus atvejus, kai 2027 m. gruodžio 11 d. arba vėliau atliekamas esminis jų pakeitimas. Dėl sąvokų „pateikimas rinkai“ ir „tiekimas rinkai“ taip pat žr. šio dokumento *2.1* skirsnį „*Pateikimas rinkai*“ ir Mėlynojo vadovo 2 skyrių.

255. Panašiai, kai produktui su skaitmeniniais elementais taikomi Reglamente (ES) 2023/1230 (Mašinų reglamente), kuris visa apimtimi taikomas nuo 2027 m. sausio 20 d., nustatyti su kibernetiniu saugumu susiję esminiai sveikatos ir saugos reikalavimai ir remiantis tais reikalavimais yra išduotas ES tipo tyrimo sertifikatas arba patvirtinimo sprendimas, toks sertifikatas ar patvirtinimo sprendimas pagal KAA 69 straipsnio 1 dalį ir toliau galioja tai kibernetinio saugumo rizikai, kurią apima Mašinų reglamentas.

256. Tai visų pirma siejama su kibernetinio saugumo aspektais, susijusiais su apsauga nuo sugadinimo ir valdymo sistemų sauga bei patikimumu, kaip nustatyta Mašinų reglamento III priedo 1.1.9 ir 1.2.1 punktuose. KAA taikymo tikslais gamintojai neprivalo dėl tokios rizikos iš naujo vertinti ar iš naujo įrodyti atitikties tol, kol atitinkamas sertifikatas ar patvirtinimo sprendimas galioja, ir bet kuriuo atveju ne ilgiau kaip iki 2028 m. birželio 11 d. Tai taikoma tiek, kiek tokia rizika buvo įvertinta atliekant atitikties vertinimą pagal Mašinų reglamentą.

257. Kaip ir minėtų RĮD esminių kibernetinio saugumo reikalavimų atveju, jei pagal KAA 13 straipsnio 2 dalį atlikus kibernetinio saugumo rizikos vertinimą nustatoma papildoma kibernetinio saugumo rizika, kurios neapima pagal Mašinų reglamentą išduotas atitinkamas sertifikatas ir kuri yra susijusi su tame reglamente nustatytais kibernetinės saugos reikalavimais, gamintojai ir toliau atsako už tokios rizikos valdymą pagal KAA.