PRIEKŠLIKUMS

Saskaņā ar Elektronisko sakaru likuma (UL RS Nr. 130/22 un 18/23 — ZDU-1O) 116. panta 6. punktu Slovēnijas Republikas Komunikāciju tīklu un pakalpojumu aģentūra, ņemot vērā informēšanas procedūru saskaņā ar Eiropas Parlamenta un Padomes 2015. gada 9. septembra Direktīvu (ES) 2015/1535, ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.), izdod šādus dokumentus:

VISPĀRĒJAIS LIKUMS
par papildu drošības prasībām un ierobežojumiem

1. pants
(Vispārējā akta saturs)

Šis vispārīgais akts paredz:

1. pamatnostādnes, kas jāievēro mobilo sakaru tīklu operatoriem (turpmāk “operatori”), kuri nodrošina šos tīklus kritiskajām vienībām, kas ir kritiskās infrastruktūras pārvaldītāji citās kritiskās infrastruktūras regulēšanas jomās, kā noteikts tiesību aktos, kas reglamentē kritiskās infrastruktūras jomu (turpmāk “kritiskās infrastruktūras pārvaldītāji”), pamatpakalpojumu sniedzējiem, kā noteikts tiesību aktos, kas reglamentē informācijas drošību (turpmāk — “pamatpakalpojumu sniedzēji”), valsts pārvaldes iestādēm, kā noteikts tiesību aktos, kas reglamentē informācijas drošību (turpmāk “valsts pārvaldes iestādes”), vai valsts drošības sistēmas galveno daļu pārvadātājiem; un
2. tīkla un saistīto informācijas sistēmu kritiskos elementus ar to funkcijām, kas minētas Elektronisko sakaru likuma 116. panta 6. punktā (UL RS Nr. 130/22 un 18/23 — ZDU-1O; turpmāk tekstā — “Akts”), kā izklāstīts pielikumā, kas ir šā vispārīgā akta neatņemama sastāvdaļa un ir sagatavots sadarbībā ar struktūru, kura ir atbildīga par informācijas drošību.

2. pants
(Terminu nozīme)

(1) Šajā vispārīgajā aktā izmantotie termini nozīmē:

1. Piegādes ķēde ir visa procesu, cilvēku, organizācijas un izplatīšanas sistēma, kas iesaistīta operatora tīklā vai mākoņpakalpojumu sniedzēja, kas sniedz šādus pakalpojumus operatoram, projektēšanā, ražošanā, uzglabāšanā, izplatīšanā un piegādē, kā arī kritiski svarīgo tīkla elementu sastāvdaļu uzstādīšanā un uzturēšanā.

2. Tīkla kritiskie elementi ir tie tīkla elementi, funkcijas, pakalpojumi un atbalsta informācijas sistēmas fiziskā, programmatūras vai virtualizētā veidā pie operatora vai mākoņpakalpojumu sniedzēja, kā uzskaitīts šā vispārīgā akta pielikumā.

3. Kritiskās struktūras ir kritiskās infrastruktūras pārvaldītāji citās kritiskās infrastruktūras regulējuma jomās, kas noteiktas saskaņā ar likumu, kas regulē kritiskās infrastruktūras jomu, būtisko pakalpojumu sniedzēji, kā noteikts informācijas drošības

likumā, valsts pārvaldes institūcijas, kā noteikts informācijas drošības likumā, un valsts drošības sistēmas galveno daļu nesēji.

(2) Citiem šajā vispārīgajā aktā izmantotajiem terminiem ir tāda pati nozīme, kā definēts Likumā un Vispārējā likumā par tīklu, pakalpojumu un datu drošību.

3. pants
(Vispārēji ieteikumi)

(1) Kritiski svarīgu tīkla elementu komponentu piegādes ķēdes operatori un šo komponentu trešā līmeņa atbalsta pakalpojumi visā šo komponentu aprites ciklā ņem vērā vismaz šādas pamatnostādnes:

1. individuālam ražotājam vai piegādātājam un trešā līmeņa atbalsta pakalpojumu sniedzējam, pamatojoties uz attiecībām un nolīgumiem ar tiem, tie veic riska novērtējumu attiecībā uz piedāvājumu un iespējamo ietekmi, ko veic trešās personas saskaņā ar publiskajām vai privātajām tiesībām (turpmāk "trešās personas"), saderību ar citu ražotāju iekārtām, produktu kvalitāti un drošību un iespējamo negatīvo ietekmi uz operatora pakalpojumu un kritisko vienību darbību;
2. ka drošība ir iestrādāta un īstenota jau projektā un ka līgumos ir noteikti termiņi šķietamās neaizsargātības novēršanai;
3. ka galvenie drošības elementi (pieejamība, konfidencialitāte, integritāte un autentiskums) tiek nodrošināti visā to izmantošanas ciklā,
4. ka tiek garantēta drošība un to nepārtraukta piegāde, un ir apstiprināts, ka tā atbalsta augstus drošības elementus saskaņā ar starptautiski atzītiem standartiem (3GPP) un Eiropas tehniskajiem standartiem (ETSI);
5. ka šā punkta 2. līdz 4. punktā minētās pamatnostādnes ir pārbaudāmas līguma dokumentācijā ar ražotāju vai piegādātāju;
6. attiecībā uz katru ražotāju vai piegādātāju tiek novērtēti un ņemti vērā arī riski, kas saistīti ar galveno tehnoloģiju izmantošanas tiesībām, kuras nepieciešamas iekārtu ražošanai un lietošanai, un riski, kas saistīti ar aprīkojuma, rezerves daļu vai trešā līmeņa atbalsta pakalpojumu piegādi;
7. ka izmantotajiem komponentiem nav neatrisinātas zināmas kritiskas vai aktīvi izmantotas neaizsargātības;
8. izvairīšanās no viena ražotāja vai piegādātāja, ja tas ir tehniski iespējams un ekonomiski ilgtspējīgi, ar mērķi samazināt atkarību un palielināt noturību gadījumā, ja trešās fiziskās vai juridiskās personas, kas ir publisko tiesību subjekti vai privāttiesību subjekti, kritiski svarīgu komponentu neaizsargātības, katastrofālas tīkla atteices vai kritisko vienību tīklu un pakalpojumu drošības apdraudējuma gadījumā.

(2) Piegādājot informācijas un sakaru iekārtas, sistēmas un pakalpojumus, operatori, iepērkot drošus IKT produktus un pakalpojumus, pilnībā ievēro Eiropas Savienības Kiberdrošības aģentūras (turpmāk "ENISA") pamatnostādnes un spēkā esošos Eiropas Savienības noteikumus par drošības pamatprasībām. Aģentūra savā tīmekļa vietnē publicē saites uz pašreizējiem ENISA dokumentiem un ES regulām minētajā jomā un pastāvīgi atjaunina tās.

(3) Piegādājot kritiski svarīgu tīkla elementu komponentus vai izmantojot mākoņpakalpojumus, prioritāti piešķir komponentu izvēlei no tiem ražotājiem vai piegādātājiem vai pakalpojumiem no mākoņpakalpojumu sniedzējiem, kurus sertificējušas

atbilstības novērtēšanas struktūras, kas ir akreditētas un vajadzības gadījumā pilnvarotas, pamatojoties uz 60. panta 3. punktu Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa Regulā (ES) 2019/881 par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju un ar ko atceļ Regulu (ES) Nr. 526/2013 (turpmāk "regula"), lai izdotu Eiropas kiberdrošības sertifikātus konkrētā apliecinājuma līmenī, kā noteikts regulas 52. pantā.

(4) Piemērojot iepriekšējo punktu, operators pārbauda īpašu tīmekļa vietni, ko ENISA izveidojusi saskaņā ar regulas 55. pantu un kuras mērķis ir informēt sabiedrību par Eiropas kiberdrošības sertifikācijas shēmām, Eiropas kiberdrošības sertifikātiem un ES atbilstības deklarācijām, tostarp informāciju par Eiropas kiberdrošības sertifikācijas shēmām, kas vairs nav derīgas vai atsauktas un kurām beidzies derīguma termiņš, un ES atbilstības deklarācijām, kā arī saišu repozitoriju ar kiberdrošības informāciju.

4. pants
(Riska novērtējums)

(1) Nosakot komponenta ražotāja vai piegādātāja un trešā līmeņa pakalpojumu sniedzēja risku attiecībā uz kritiski svarīgiem tīkla elementiem, operators ņem vērā šādus riska aspektus, kurus tas novērtē.

(2) Iepriekšējā punktā minētajā novērtējumā operators novērtē un ņem vērā vismaz:

1. vispārējo kvalitāti (tostarp drošības aspektus) un uzticamību;
2. tādu atvērtu standartu un saskarņu izmantošanas līmeni, kas novērš atkarību un piesaisti konkrēta ražotāja vai piegādātāja ražojumiem;
3. atbilstību atzītiem starptautiskajiem un Eiropas tehniskajiem standartiem (3GPP, ETSI) un Eiropas Savienības noteikumiem un noklusējuma drošības iestatījumiem saskaņā ar profesionālajiem ieteikumiem (GSMA asociācija);
4. saderības līmeni ar trešo personu iekārtām un tīkla funkcijām;
5. spēju nodrošināt uzlabojumus un pielāgojumus;
6. neaizsargātības pārvaldības procesus, to atklāšanu un atjauninātu procesu ar atjauninājumiem un labojumiem;
7. dokumentu pieejamību un pārredzamību attiecībā uz:
   - galvenajām funkcijām un informāciju par komponenta drošību un citiem elementiem un iespējamiem iestatījumiem, un
   - izmantoto programmatūru, tostarp atvērto pirmkodu (materiālu likumprojekts — SBOM);
8. atkarības līmeni no trešā līmeņa atbalsta pakalpojumiem iekārtu pārvaldībā un apkopē, ja operators šos pakalpojumus nesniedz viens pats ar saviem darbiniekiem;
9. sākotnējo novērtējumu par tāda aprīkojuma vai subjekta atbilstību, kas sniegtu trešā līmeņa atbalsta pakalpojumus, ko veic struktūras, kuras akreditētas Eiropas Savienībā saskaņā ar Eiropas kiberdrošības sertifikācijas shēmām, un saskaņā ar kuru akreditētās struktūras tiek publicētas Eiropas Savienības *Oficiālajā Vēstnesī*.

(3) Operators dokumentē riska faktorus un riska novērtējuma rezultātus katram izvēlētajam ražotājam vai piegādātājam, vai trešā līmeņa pakalpojumu sniedzējam, kas minēts šā panta 2. un 3. punktā, un regulāri to atjaunina.

5. pants
(Vispārējas pamatnostādnes par kritiski svarīgu tīkla elementu ekspluatāciju)

(1) Kritisko tīkla elementu komponenti, to darbība un noklusējuma iestatījumi neietver tehniskus raksturlielumus, kas varētu negatīvi ietekmēt kritisko vienību drošību vai darbību, cita starpā sabotāžas, spiegošanas, intelektuālā īpašuma zādzības vai terorisma dēļ.

(2) Kritiskie tīkla elementi parasti atrodas Slovēnijas Republikā vai, ņemot vērā visus drošības riskus un nodrošinot augsta līmeņa drošības pasākumus, un, ja piemērojamos noteikumos tas nav noteikts citādi, Eiropas Savienībā. Operators vismaz 30 dienas pirms pārcelšanas ārpus Eiropas Savienības informē Slovēnijas Republikas Komunikācijas tīklu un pakalpojumu aģentūru (turpmāk "Aģentūra") un par informācijas drošību atbildīgo struktūru par paredzēto pārcelšanu.

(3) Trešā līmeņa atbalsta pakalpojumi kritiski svarīgiem tīkla elementiem parasti tiek sniegti Slovēnijas Republikā vai, ņemot vērā visus drošības riskus un nodrošinot augsta līmeņa drošības pasākumus, un, ja piemērojamos noteikumos tas nav noteikts citādi, Eiropas Savienībā. Operators vismaz 30 dienas pirms pārcelšanas ārpus Eiropas Savienības valstīm paziņo Aģentūrai un par informācijas drošību atbildīgajai struktūrai par savu trešā līmeņa atbalsta dienestu plānoto pārcelšanu.

(4) Trešā līmeņa atbalsta pakalpojumu īstenošana neapdraud kritisko vienību pakalpojumu drošību vai darbību vai valsts drošību.

(5) Operators izveido un regulāri īsteno kritiski svarīgo tīkla elementu noteikšanas procesu. Tas jāveic vismaz reizi gadā vai tad, kad tiek iepirkti kritiski svarīgu tīkla elementu komponenti.

(6) Ja atsevišķs komponents tikai daļēji pārstāv kritisko tīkla elementu, to uzskata par kritiskā tīkla elementa daļu.

(7) Operators uztur atjauninātu sarakstu ar visiem kritiski svarīgo tīkla elementu komponentiem, to funkcijām, atrašanās vietām, administratoriem un vadītājiem, trešā līmeņa atbalsta pakalpojumu sniedzējiem un to ražotājiem vai piegādātājiem. Pēc pieprasījuma sarakstu dara pieejamu Aģentūrai un par informācijas drošību atbildīgajai struktūrai.

6. pants
(Drošības pasākumi kritiski svarīgu tīkla elementu komponentu piegādei)

(1) Operators ir informēts par visu piegādes ķēdi un ar to saistītajiem riskiem, tostarp par kritiski svarīgu tīkla elementu atsevišķu komponentu apakšuzņēmējiem, kas ietver arī šifrēšanas atslēgas, UICC/eUICC un citus drošības elementus, kuru ļaunprātīga izmantošana varētu apdraudēt kritisko vienību drošību.

(2) Operators nodrošina, ka drošības prasības starp operatoru un kritiski svarīgu tīkla elementu komponentu ražotājiem vai piegādātājiem vai tā trešā līmeņa atbalsta pakalpojumu sniedzējiem ir līgumā noteiktas un dokumentētas, un pieprasa, lai ražotāji vai piegādātāji ievērotu saskaņotos drošības pasākumus visā piegādes ķēdē.

(3) Lai novērstu to, ka ļaunprātīgi dalībnieki laikus izmanto vājās vietas, operators nodrošina, ka kritiski svarīga tīkla elementa komponentu ražotājs vai piegādātājs līgumā apņemas nekavējoties informēt operatoru par konstatēto neaizsargātību un par riska mazināšanas pasākumiem un konsultēt par aizsardzības vai korektīviem pasākumiem, ko operators var veikt, reaģējot uz apdraudējumu.

(4) Operators vismaz reizi gadā pārbauda piekļuves tiesību atbilstību kritiski svarīgiem tīkla elementiem vai tās nekavējoties atjaunina saskaņā ar izmaiņām organizācijā vai trešā līmeņa atbalsta pakalpojumu sniedzēju pusē.

(5) Operators novērš savu atkarību no atsevišķa piegādātāja vai trešā līmeņa pakalpojumu sniedzēja (t. i., "pārdevēja piesaiste"), ja tas ir tehniski iespējams un ekonomiski ilgtspējīgs, lai mazinātu atkarību un palielinātu noturību kritiski svarīgu komponentu ievainojamības gadījumā, arī izvairoties no ilgtermiņa līgumiem ar atsevišķiem ražotājiem vai piegādātājiem vai trešā līmeņa atbalsta pakalpojumu sniedzējiem, vai iespēju tos mainīt, lai samazinātu traucējumus pakalpojumu sniegšanā kritiskajām vienībām līdz zemākajam iespējamajam līmenim.

7. pants
(Līgumu noteikumi ar ražotājiem, piegādātājiem vai trešā līmeņa atbalsta pakalpojumu sniedzējiem)

Lai nodrošinātu augstu drošības līmeni, operators jaunajos līguma noteikumos ar ražotājiem, piegādātājiem vai trešā līmeņa atbalsta pakalpojumu sniedzējiem iekļauj vismaz šādu informāciju:

1. ražotāja vai piegādātāja paziņojumu, ka komponentam vai tā noklusējuma iestatījumiem nav ne dokumentētu aizmugurdurvju, ne negatīvas ietekmes uz kritisko vienību darbību;
2. ražotāja, piegādātāja vai trešā līmeņa pakalpojumu sniedzēja apņemšanos aizsargāt datus, ar kuriem tie iepazīstas, sniedzot pakalpojumus vai piekļūstot tiem saistībā ar piekļuves pakalpojuma sniegšanu;
3. ražotāja, piegādātāja vai trešā līmeņa pakalpojumu sniedzēja apņemšanos nekavējoties informēt operatoru par komunikācijas datu vai datu plūsmas aizsardzības pārkāpumiem, kas ietekmē vai varētu ietekmēt operatoru vai šā vispārīgā akta 1. panta 1. punktā minētās kritiskās vienības;
4. ražotāja, piegādātāja vai trešā līmeņa pakalpojumu sniedzēja apņemšanos nekavējoties informēt operatoru par jebkuru drošības incidentu un ievainojamību, kas varētu ietekmēt tīkla, saistīto pakalpojumu vai operatora datu drošību;
5. ražotāja, piegādātāja vai trešā līmeņa pakalpojumu sniedzēja apņemšanos ievērot operatora noteiktos drošības standartus un noteikumus un veikt atbilstīgus drošības pasākumus, lai nodrošinātu informācijas sistēmu un tīklu un operatora vai kritiskās vienības datu drošību;
6. operatora spēju jebkurā laikā pārskatīt vidi, procedūras, drošības pasākumus un rīkus, ko izmanto trešā līmeņa atbalsta pakalpojumu sniedzējs, piekļūstot operatora tīklam un datiem;
7. ražotāja vai piegādātāja, vai trešā līmeņa atbalsta pakalpojumu sniedzēja atbildību par kaitējumu, ko izraisītu konstatētas ievainojamības vai kritiski svarīgu tīkla elementu komponentu ļaunprātīga izmantošana, to noklusējuma iestatīšana vai tādu

trešā līmeņa atbalsta pakalpojumu sniegšanas laikā, kurus ražotājs vai piegādātājs, vai trešā līmeņa atbalsta sniedzējs ir atstājis novārtā vai apzināti īstenojis;

8. pienākumu regulāri apmācīt ražotāja vai piegādātāja vai trešā līmeņa atbalsta pakalpojumu sniedzēja personālu datu drošības un informācijas sistēmu un tīklu jomā.

8. pants
(Noteikumi par piekļuvi kritiski svarīgiem tīkla elementiem un to izmantošanu)

(1) Fiziski vai loģiski piekļūstot kritiski svarīgu tīkla elementu komponentiem, to iestatījumiem un tajos glabātajiem, apstrādātajiem vai pārveidotajiem operatora datiem, operators nodrošina, ka:

1. piekļuve ir stingri ierobežota, attiecinot to tikai uz personām, kurām iepriekš ir piešķirta atļauja;
2. visus uz vietas vai ar attālinātu piekļuvi veiktos kritiski svarīgos tīkla elementus kontrolē operators;
3. daudzfaktoru autentificēšanu veic lietotājiem, kuriem ir piešķirtas vislielākās tiesības piekļūt kritiski svarīgu tīkla elementu atsevišķiem komponentiem, to iestatījumiem vai tur glabātajiem vai apstrādātajiem datiem;
4. katrai pilnvarotai personai, kurai ir piešķirta piekļuve, ir unikāls lietotāja konts un parole;
5. tiek izmantotas tikai tās paroles, kuras regulāri vai nekavējoties maina nepareizas lietošanas gadījumā un kurās ir vismaz 15 rakstzīmes un kurās ir iekļauti lielie un mazie burti, cipari un īpašas rakstzīmes, ja programmatūra to atļauj;
6. attiecībā uz piekļuvi, ja iespējams, tiek īstenots pilnīgas neiecietības vai uzticēšanās jēdziens;
7. autorizētā lietotāja saziņas savienojuma ar atsevišķiem komponentiem drošība tiek aizsargāta, izmantojot šifrēšanu, ņemot vērā jaunākos tehnoloģiskos sasniegumus un labāko rūpniecisko paraugpraksi informācijas drošības jomā, vai to iesaka informācijas drošības jomā izveidotās iestādes;
8. tiek veikta neizdzēšama piekļuves un piekļuves mēģinājumu uzskaite, kas tiek glabāta vismaz 6 mēnešus, tostarp rezerves kopija, bet var būt arī ilgāk, ja riska pārvaldības analīze un pieņemamā riska līmeņa novērtējums liecina, ka riski būtu pienācīgi jāpārvalda, glabājot reģistrus ilgākā laikposmā;
9. ja iespējams, reģistrē un uzrauga visas programmatūras intervences attiecībā uz komponentiem, tostarp konfigurācijas izmaiņas. Ierakstus, tostarp šo datu rezerves kopiju, glabā tik ilgi, cik norādīts iepriekšējā punktā;
10. piekļuve atsevišķiem komponentiem un tajos glabātajiem vai apstrādātajiem datiem ir ierobežota laikā un atvērta tikai nepieciešamā darba laikā.

(2) Ja trešā līmeņa atbalsta pakalpojumu sniedzēja personāls vai darbinieki piekļūst kritiski svarīgu tīkla elementu atsevišķiem komponentiem, tie:

1. izmanto tikai drošu starpposma darbstaciju (“pārlēkšanas serveri”), kurai veic regulāras drošības pārbaudes;
2. īpašā darbstacijā uzstāda tikai absolūti nepieciešamos rīkus, komponentus un aktīvos pakalpojumus, lai piekļūtu citiem tīkla resursiem, kas ir absolūti nepieciešami un ir jāatjaunina ar jaunākajiem drošības ielāpiem;
3. izmanto drošas kriptogrāfijas darbības un atslēgas īpašā darbstacijā, kurai jāatrodas operatora tīklā un kas atrodas vienīgi tā kontrolē;
4. katru piekļuvi operators apstiprina un aktivizē manuāli un tikai uz piekļuves laiku;

5. visas piekļuves un darbības fiziski kontrolē un reģistrē operators;
6. izmanto divfaktoru autentifikāciju un paroles, kas ir vismaz 15 rakstzīmes garas un ietver lielos un mazos burtus, ciparus un īpašas rakstzīmes, kuras maina, pamatojoties uz novērtētajiem riskiem.

(3) Pirms operators nodod kritiski svarīgu tīkla elementu vai to atsevišķo komponentu pārvaldības, uzturēšanas vai atjaunināšanas pakalpojumu trešai personai, tas pārbauda un nodrošina, ka tam ir vismaz tādi paši vai labāki drošības mehānismi un drošības pārvaldības procesi salīdzinājumā ar tā mehānismiem un procesiem. Par nodomu veikt pārsūtīšanu tas nekavējoties informē attiecīgo kritisko vienību, Aģentūru un par informācijas drošību atbildīgo struktūru.

(4) Operators pārbauda drošības procesu faktisko stāvokli pirms pakalpojumu sniegšanas sākuma un pēc tam vismaz reizi gadā. Operators veic uzskaiti par iekšējo pārskatīšanu un kontroli attiecībā uz trešo personu atbalsta pakalpojumu sniegšanu un glabā to visu pakalpojumu sniegšanas laiku un vienu gadu pēc to izbeigšanas, bet ne ilgāk kā piecus gadus.

PĀREJAS UN NOBEIGUMA NOTEIKUMI

9. pants
(Pārejas noteikumi)

(1) Operators 30 dienu laikā pēc šā vispārīgā akta stāšanās spēkā paziņo Aģentūrai un par informācijas drošību atbildīgajai struktūrai par kritisko tīkla elementu atrašanās vietām.

(2) Operators 30 dienu laikā pēc šā vispārīgā akta stāšanās spēkā paziņo Aģentūrai un par informācijas drošību atbildīgajai struktūrai par esošām trešā līmeņa atbalsta pakalpojumu vietām attiecībā uz kritiski svarīgiem tīkla elementiem.

(3) Aģentūra pirmo reizi publicē šā vispārīgā akta 3. panta 2. punktā minētos dokumentus no tā spēkā stāšanās dienas.

10. pants
(Stāšanās spēkā)

Šis vispārīgais akts stājas spēkā trīsdesmitajā dienā pēc tā publicēšanas Slovēnijas Republikas Oficiālajā Vēstnesī, kurā operatori var izmantot aprīkojumu un uzturēt trešā līmeņa atbalsta pakalpojumu sniegšanu līdz likuma 312. panta 2. un 3. punktā noteikto termiņu beigām.

Nr. _____ mag. Marko

Mišmaš

Ljubljana, (datums) _____ direktors

EVA 2023-3150-0034

PRIEKŠLIKUMS

PRIEKŠLIKUMS

Pielikums

Kritisko tīkla elementu un saistīto informācijas sistēmu saraksts:

Kritiskie tīkla elementi	**Tīkla un informācijas sistēmu funkcijas**
Abonentu pārvaldības un šifrēšanas mehānismi	- Sesijas vadība (balss un dati), - lietotāju un iekārtu autentificēšanu tīklā, - abonentu un tīkla komponentu atļauju atslēgu pārvaldība un glabāšana (UICC/eUICC, digitālie sertifikāti/HSM), - funkcijas drošai autentifikācijai, saziņas integritātes aizsardzībai (šifrēšanai) un lietotāja atslēgu, tīkla un pārvaldības komponentu uzglabāšanai, - piekļuves tiesību pārvaldība.
Starpsavienojums	- Mitināšanas funkcijas un saskarnes ar citiem tīkliem un pakalpojumiem.
Pārvaldīti tīkla pakalpojumi	- Tīkla pakalpojumu reģistrēšana un atļaušana, - sakaru, atrašanās vietas un datu plūsmas datu glabāšana un apstrāde, - tīkla un tīkla funkciju pakļaušana ārējām lietojumprogrammām un pakalpojumiem.
Virtualizēto tīkla funkciju (NFV) un tīkla orķestrācijas (MANO) pārvaldība un organizēšana, tostarp virtualizācijas infrastruktūra	- NFV orķestrācijas un konfigurācijas vadības funkcijas neatkarīgi no īstenošanas veida (VM, konteineri, mikropakalpojumi), - virtualizācijas funkcijas NFV ieviešanai un izmantošanai, - tīkla sadaļu atlases funkcija (NSSF);
Radiopiekļuves tīkls	- Bāzes stacijas, kas atbalsta 5G tehnoloģiju vai augstāku.
Pārvaldības sistēmas un citas atbalsta sistēmas	- Mobilo sakaru tīkla, tostarp piekļuves daļas (RAN/O-RAN), darbības un pārvaldības uzraudzība, - sistēmas drošības notikumu, anomāliju, draudu atklāšanai un to pārvaldībai (drošības funkcijas, tostarp SIEM/SOAR).
Juridiskā pārtveršana	- Funkcijas, kas saistītas ar kompetentās iestādes piekļuvi saziņas saturam un datiem par lietotāju datplūsmu.