BIEŽĀK UZDOTIE JAUTĀJUMI

Aizsardzības ministrijas Kiberdrošības politikas departaments ir apkopojis biežāk uzdotos jautājumus par Nacionālās kiberdrošības likuma (NKDL) un Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" (MK noteikumi Nr. 397) piemērošanu.

SUBJEKTU PAŠIDENTIFIKĀCIJAS JAUTĀJUMI

1. Kā var pārliecināties par atbilstību NKDL statusam?

Aicinām izmantot izstrādāto interaktīvo rīku – testu, kas palīdzēs noteikt, vai NKDL izpratnē Jūsu pārstāvētā organizācija uzskatāma par subjektu un uz to attiecas no normatīvajiem aktiem izrietošie pienākumi. Norādām, ka tests ir indikatīvs un var atšķirties no faktiskās situācijas, līdz ar to, ja pēc testa aizpildīšanas nav iegūta pārliecība par atbilstību vai rodas papildu jautājumi, aicinām sazināties ar NIS2 kontaktpunktu: NIS2@mod.gov.lv.

2. Vai iestāde var vienlaikus būt gan būtisko, gan svarīgo pakalpojumu sniedzējs, gan IKT kritiskās infrastruktūras turētājs?

Kaut arī iestāde var atbilst gan būtisko pakalpojumu sniedzēja, gan svarīgo pakalpojumu sniedzēja pazīmēm, kā atbilstošo nosaka augstāko.

Gadījumā, ja attiecībā uz pakalpojuma sniedzēju vienlaicīgi izpildās būtisko pakalpojumu sniedzēja un svarīgo pakalpojumu sniedzēja pazīmes, šāds pakalpojuma sniedzējs NKDL izpratnē uzskatāms par būtisko pakalpojumu sniedzēju. Piemēram, valsts dibināta augstskola, kas vienlaikus ir atvasināta publiska persona un izglītības informācijas sistēmas uzturētājs, NKDL izpratnē uzskatāma par būtisko pakalpojumu sniedzēju.

Ja iestāde atbilst vairākām NDKL noteikto subjektu kategorijām, tai reģistrējoties NKDC, tāpat jānorāda visas atbilstošās darbības jomas (gan būtiskās, gan svarīgās).

Augstāk minētajos gadījumos NKDL subjektu uzraudzību veic Nacionālais kiberdrošības centrs (NKDC).

Savukārt, ja iestāde ir būtisko pakalpojumu sniedzējs vai svarīgo pakalpojumu sniedzējs, bet tā īpašumā vai valdījumā ir IKT kritiskā infrastruktūra, tam piemēro IKT kritiskajai infrastruktūrai noteiktās prasības un tā uzraudzību veic SAB. Vienlaikus, iestādei ir jāreģistrējas NKDC kā attiecīgi būtisko pakalpojumu sniedzējam vai svarīgo pakalpojumu sniedzējam.

Ņemot vērā iepriekš minēto, iestāde nevar vienlaicīgi būt būtisko pakalpojumu sniedzējs un svarīgo pakalpojumu sniedzējs, bet tā var vienlaicīgi būt būtisko pakalpojumu sniedzējs vai svarīgo pakalpojumu sniedzējs un IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

3. Kas uzraudzīs kiberdrošību subjektā, ja tā valdījumā ir sistēma, kas ir IKT KI?

Šādā gadījumā uzraudzību veiks SAB.

4. Vai pēc būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapas iesniegšanas tiks saņemts kāds paziņojums, lēmums vai informatīva vēstule par subjekta iekļaušanu šajā sarakstā?

NKDC informēs subjektu par anketas saņemšanu, nepieciešamo papildu informāciju, ja tāda būs, iekļaušanu sarakstā, kā arī atgādinās arī par nākamajiem informācijas iesniegšanas termiņiem.

5. Vai visi vidēji saimnieciskās darbības veicēji, kuri uztur tiešsaistes tirdzniecības vietu, ir tiešsaistes tirdzniecības vietas pakalpojumu sniedzēji saskaņā ar NKDL?

Nē, saskaņā ar NIS2 Direktīvu un Negodīgas komercprakses aizlieguma likumu, tiešsaistes tirdzniecības vieta ir pakalpojuma sniegšanas vieta, izmantojot programmatūru, tostarp tīmekļa vietne, tīmekļa vietnes daļa vai lietotne, ko uztur komercprakses īstenotājs vai kas tiek uzturēta komercprakses īstenotāja vārdā un kas ļauj patērētājiem slēgt distances līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai patērētājiem. Attiecīgi tiešsaistes tirdzniecības vietas pakalpojumu sniedzējs ir tikai tādas platformas uzturētājs, kurā patērētājam ir iespēja slēgt līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai citiem patērētājiem, nevis ar pašu interneta vietnes uzturētāju.

6. Vai uzņēmums, kura pamatdarbības joma ietver impregnēšanu, ir uzskatāms par NKDL subjektu atbilstoši NKDL 20. un 21. pantā aptvertajam nozaru lokam?

Norādām, ka impregnēšana neietilpst nevienā no NKDL 20. un 21. pantā ietvertajām nozarēm. Vienlaikus norādām, ka NKDC ir analoģiski vērtējis vairākus gadījumus, kuros uzņēmuma pamatdarbība ietver impregnēšanu un secinājis, ka, piemēram, koksnes impregnēšana nevar tikt pielīdzināta ķīmisko vielu ražošanai, jo impregnēšanas procesā koksne tiek tikai apstrādāta ar kāda cita komersanta ražotu ķīmisko vielu, kā rezultātā netiek mainīts koksnes molekulārais sastāvs un pati koksne kā materiāls nekļūst par ķīmisko vielu. Tādējādi neveidojas jauns ķīmiskais elements, kā tas notiek ražošanas procesā, līdz ar to impregnēšana neatbilst nevienai no NKDL 20. un 21. pantā ietvertajām nozarēm un nav uzskatāma par būtisko pakalpojumu vai svarīgo pakalpojumu NKDL izpratnē.

7. Vai uzņēmums tiek uzskatīts par NKDL subjektu, ja tas darbojas kādā no likumā minētajām nozarēm, taču šī nav tā galvenā nozare (pamatdarbība)?

Jā, uzņēmums var tikt uzskatīts par NKDL subjektu arī tad, ja tā darbība kādā no likumā minētajām nozarēm nav tā pamatdarbība. Katram uzņēmumam ir individuāli jāizvērtē, vai tā veiktā saimnieciskā darbība ietilpst NKDL noteiktajās jomās. NKDC, vērtējot uzņēmuma atbilstību likuma subjektam, balstās uz publiski pieejamo informāciju par uzņēmumu. Papildus jāņem vērā izņēmums pārtikas nozarē — šajā gadījumā par NKDL subjektiem tiek uzskatīti tikai tie komersanti, kuru pamatdarbība ir pārtikas rūpnieciska ražošana, pārstrāde vai vairumtirdzniecības izplatīšana.

8. Vai degvielas uzpildes stacijas klasificējas kā būtisko pakalpojumu sniedzēji?

Saskaņā ar NKDL būtiskie pakalpojumu sniedzēji ir tie, kuru darbības pārtraukums būtiski ietekmētu sabiedrības drošību, veselību, ekonomiku vai valsts pārvaldes nepārtrauktību un to apgrozījums un izmērs atbilst NKDL 1. panta 16. un 25. punktam. Degvielas uzpildes stacijas kā atsevišķi komersanti parasti netiek klasificēti kā būtisko pakalpojumu sniedzēji. Tomēr, ja tās ir daļa no enerģētikas nozares kritiskās infrastruktūras (piemēram, degvielas loģistikas, uzglabāšanas un piegādes ķēdes, kas nodrošina valsts apgādi ar degvielu), tad konkrēti uzņēmumi vai to tīkli var tikt atzīti par būtisko pakalpojumu sniedzējiem atbilstoši NKDL 20. panta 11. punktam.

Vēršam uzmanību uz NKDL 20. panta 8. punktā izmantoto terminu "naftas apgādes komersants". Saskaņā ar NIS2 direktīvas I pielikuma 1. punkta c) apakšpunktu, kas nosaka ka NIS2 direktīvas attiecas arī uz naftas pārvades cauruļvadu operatoriem, naftas ražošanas, pārstrādes un attīrīšanas iekārtu operatoriem, uzglabāšanas un pārvades dalībniekiem, kā arī centrālajai krājumu uzturēšanas struktūrai. Saskaņā ar Padomes Direktīvas 2009/119/EK (2009. gada 14. septembris), ar ko dalībvalstīm uzliek pienākumu uzturēt jēlnaftas un/vai naftas produktu obligātas rezerves 2. panta f) apakšpunktu par centrālo krājumu uzturēšanas struktūru ir uzskatāma organizācija vai dienests, kuram var uzticēt pilnvaras rīkoties, lai iegādātos, uzturētu vai pārdotu naftas krājumus, tostarp drošības rezerves un īpašos krājumus.

SODI

Sodi tiek noteikti atbilstoši Ministru kabineta 2025. gada 29. aprīļa noteikumiem Nr. 252 "Noteikumi par kārtību, kādā nosakāms finanšu gada neto apgrozījums, no kura aprēķina soda naudu, un soda naudas apmēra noteikšanas kritērijiem"

9. Kā soda valsts iestādes par neatbilstībām? Vai valsts iestāžu vadītājiem neatbilstību gadījumā piespriestu naudas sodu?

Attiecībā uz valsts iestāžu vadītājiem neatbilstību gadījumā netiek piemērots naudas sods. Ja NKDL subjekts, kurš ir tiešās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, NKDC par šo neatbilstību ziņo attiecīgajam Ministru kabineta loceklim. Šādā gadījumā Ministru kabineta loceklis izvērtē nepieciešamību ierosināt disciplinārlietu un lemj par turpmāko rīcību neatbilstības novēršanai, savukārt atbildīgais Ministru kabineta loceklis par neatbilstības novēršanas gaitu ziņo Ministru kabinetam. Ja NKDL subjekts, kurš ir pašvaldība vai pašvaldības dibināta pastarpinātās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, NKDC par šo neatbilstību ziņo Viedās administrācijas un reģionālās attīstības ministram, kā arī attiecīgās pašvaldības domes priekšsēdētājam, kurš lemj par pašvaldību institūciju un amatpersonu (darbinieku) atbildību Pašvaldību likumā noteiktajā kārtībā. Vienlaikus, ja NKDL subjekts, kurš ir iepriekš neminēta valsts vai pašvaldības institūcija, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, NKDC par konstatēto neatbilstību ziņo Ministru kabinetam un Ministru kabinets lemj par turpmāko rīcību neatbilstības novēršanai.

10. Kādi ir naudas sodi par likuma prasību neievērošanu?

Attiecībā uz privāto tiesību juridiskajām personām, sankcijas par prasību neizpildi ietver soda naudas piemērošanu un administratīvā akta piespiedu izpildi. Attiecībā uz būtisko pakalpojumu sniedzējiem un IKT kritisko infrastruktūru, soda naudu var piemērot līdz 10 milj. *euro* vai līdz 2 % no uzņēmuma kopējā gada apgrozījuma pasaulē. Attiecībā uz svarīgo pakalpojumu sniedzējiem – līdz 7 milj. *euro* vai līdz 1,4 % no kopējā gada apgrozījuma pasaulē.

Vienlaikus, NKDC un SAB atbilstoši NKDL noteiktajam, veicot uz noteiktu darbību vai darbības aizliegumu vērsta lēmuma piespiedu izpildi, ir tiesības uzlikt piespiedu naudas sodu, kas vienā reizē nepārsniedz 10 000 *euro*.

PRASĪBAS KIBERDROŠĪBAS PĀRVALDNIEKAM

11. Vai kiberdrošības pārvaldnieks var būt uzņēmuma IT departamenta pārstāvis?

Jā, lai gan saskaņā ar labās prakses principiem, lai mazinātu iespējamu interešu konfliktu, par kiberdrošības pārvaldību atbildīgajai personai būtu jāatrodas tiešā uzņēmuma vai iestādes vadītāja pakļautībā, par pārvaldnieku drīkst būt nozīmēts arī IT departamenta pārstāvis. Tas gan neatbilst labās prakses principiem, jo šādā gadījumā kiberdrošības pārvaldnieks pēc būtības var netieši novērtēt arī organizācijas IT uzturētāju (tai skaitā savu) darbu. Vienlaikus jāuzsver, ka par kiberdrošību organizācijā kopumā atbild tās vadītājs, un kad tiek iecelts kiberdrošības pārvaldnieks, tam jāsadarbojas tieši ar organizācijas vadītāju, nevis IT departamenta direktoru.

12. Vai kiberdrošības pārvaldnieku var nolīgt ārpakalpojumā?

Jā, subjekts var piesaistīt kiberdrošības pārvaldības ārpakalpojumus, nodrošinot kiberdrošības prasībām atbilstošu kontroli. Vienlaikus ir jāņem vērā, ka IKT KI īpašniekam vai tiesiskajam valdītājam kiberdrošības pārvaldnieka pretendents ir jāsaskaņo ar SAB.

13. Cik subjektos kiberdrošības pārvaldnieks var strādāt vienlaicīgi?

MK noteikumu Nr. 397 17.-19. punktā ir noteikts, cik subjektos viena fiziskā persona var vienlaicīgi būt kiberdrošības pārvaldnieks.

Detalizētāk izšķiramas 4 situācijas:

- Svarīgo pakalpojumu sniedzējos – neierobežotā skaitā;
- Būtisko pakalpojumu sniedzējos (kas nav IKT KI) – piecos subjektos;
- B un C kategorijas IKT KI – vienā IKT KI (+ piecos būtisko pakalpojumu sniedzējos + neierobežotā skaitā svarīgo pakalpojumu sniedzēju);
- A kategorijas IKT KI – tikai vienā subjektā.

Papildu iepriekš minētajam MK noteikumu Nr. 397 19. punkts pieļauj pārsniegt būtisko pakalpojumu sniedzēju (ja tie nav IKT KI) skaita ierobežojumu, ja visi subjekti ir savstarpēji

saistīti 19. punktā aprakstītajos padotības veidos. Jāņem vērā, ka saistītie subjekti netiek uzskatīti par vienu subjektu – katrs subjekts tik un tā tiek uzskaitīts atsevišķi.

Piemēram, ja kiberdrošības pārvaldnieks strādā būtisko pakalpojumu sniedzējā un vēl septiņos tā meitas uzņēmumos (kas arī būtisko pakalpojumu sniedzēji), uzskatāms, ka pārvaldnieks pilda pienākumus astoņos būtisko pakalpojumu sniedzējos, nevis vienā. Saskaņā ar MK noteikumu Nr.397 19. punktu tas ir pieļaujams.

Taču šādā gadījumā pārvaldnieks vairs nedrīkst uzņemties pienākumus citā nesaistītā (devītajā) būtisko pakalpojumu sniedzējā, jo: a) tiktu pārsniegts 18. punkta ierobežojums (ne vairāk kā pieci būtisko pakalpojumu sniedzēji); b) 19. punktā paredzētais izņēmums attiecībā uz šo būtisko pakalpojumu sniedzēju nav piemērojams, jo šis subjekts neietilpst iepriekš minētās uzņēmumu grupas ietvaros, t.i. tam nav savstarpējas saistības ar citiem pārvaldnieka subjektiem.

14. Kā ir drošāk – ņemt kiberdrošības pārvaldnieka ārpakalpojumu vai sūtīt savu darbinieku uz kiberdrošības sertifikācijas kursiem?

MK noteikumi Nr. 397 paredz, ka katram subjektam ir jānodrošina atbilstoša kiberdrošības pārvaldība, ņemot vērā informācijas resursu klasifikāciju, piemērojamos aizsardzības pasākumus un speciālo regulējumu prasības. Līdz ar to izvēle starp ārpakalpojumu un iekšējā darbinieka apmācību ir jāveic, balstoties uz riska novērtējumu un organizācijas vajadzībām ilgtermiņā. Ārpakalpojuma izmantošana nodrošina ērtu piekļuvi kompetencei un resursiem, taču samazina tiešu iekšējo kontroli pār kiberdrošības procesiem. Iekšējā darbinieka apmācība un sertifikācija ilgtermiņā ir drošāks risinājums, jo zināšanas un kompetence veidojas un attīstās organizācijā, t.sk. ņemot vērā aktuālos kiberriskus attiecīgajā darbības jomā. Praksē ir novērota kombinēta pieeja: pārejas periodā izmantot ārpakalpojumu, vienlaikus ieguldot sava darbinieka profesionālajā attīstībā (piem., CISSP, CISM, ISO/IEC 27001 sertifikācijas iegūšanā), lai nodrošinātu ilgtspējīgu kiberdrošības pārvaldību.

15. Kāda izglītība nepieciešama kiberdrošības pārvaldniekam? Kādi starptautiskie kursi vai sertifikāti ir nepieciešami/derīgi?

Atbilstoši MK noteikumu Nr. 397 3.1. apakšnodaļai par kiberdrošības pārvaldnieku var strādāt fiziska persona, kurai ir augstākā vai vidējā profesionālā izglītība IT, kiberdrošības pārvaldības vai citā saistītā jomā, vai kura ir saņēmusi starptautiski atzītu sertifikātu, kas apliecina personas kvalifikāciju kiberdrošības pārvaldības jomā (piemēram, CISM, CISSP), vai kurai ir vismaz divu gadu darba pieredze kiberdrošības pasākumu plānošanā vai īstenošanā, kas iegūta pēdējo 5 gadu laikā. Līdz ar to ir jāizpildās vismaz vienam no iepriekš uzskaitītajiem kritērijiem, lai persona varētu tikt iecelta par kiberdrošības pārvaldnieku subjektā.

Saskaņā ar MK noteikumu Nr. 397 11.5., 12.3. un 13.3 apakšpunktā noteikto viens no kiberdrošības pārvaldnieka kompetences apliecinājumiem var būt arī starptautiski atzīts sertifikāts kiberdrošības pārvaldībā. Šajā ziņā par atbilstošu tiktu uzskatīts jebkurš no starptautiski zināmiem sertifikātiem tieši ar uzsvaru kiberdrošības pārvaldības pasākumu veikšanā. Kā dažus piemērus varam minēt: CISSP, CISM, CISA, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer un CompTIA Security+. Protams, pieļaujama kvalifikācijas iegūšana citās sertifikācijas iestādēs un ar citiem sertifikātiem, bet galvenajam uzsvaram būtu jābūt tieši uz kiberdrošības pārvaldību.

16. Vai kiberdrošības pārvaldnieks var būt Latvijas nepilsonis?

Nē. Saskaņā ar MK noteikumu Nr. 397 12. un 13. punktā noteikto par kiberdrošības pārvaldnieku būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējā var būt fiziska persona, kurai ir NATO, Eiropas Savienības vai Eiropas Brīvās tirdzniecības asociācijas valsts pilsonība. Par kiberdrošības pārvaldnieku IKT kritiskās infrastruktūras īpašniekā vai tiesiskajā valdītājā drīkst būt tikai Latvijas pilsonis.

17. Vai kiberdrošības pārvaldnieka pienākumus var veikt vairākas personas vai komanda, nevis tikai viena konkrēta persona?

Nē, kiberdrošības pārvaldnieks nevar būt komanda kopumā – par kiberdrošības pārvaldnieku tiek iecelta konkrēta persona vai personas. Ir iespējams arī iecelt divas personas. Vienlaikus subjekta atbildībā ir noteikt uzdevumu un darbu sadalījumu starp šīm noteiktajām personām, un noteikt kā tiek sadalīta atbildība savstarpēji sadalot atbildības jomas un pienākumus. Vienlaikus atsevišķus kiberdrošības pasākumus (piemēram, rezerves kopiju vai žurnālfailu veidošanu) var veikt arī vairāki darbinieki, taču atbildība par šo pasākumu izpildi saglabājas kiberdrošības pārvaldniekam(-iem).

18. Vai globālā (Šveices) uzņēmuma Informācijas drošības departamenta pārstāvis var būt iecelts kā kiberdrošības pārvaldnieks Latvijas uzņēmumā?

Globālā uzņēmuma (piemēram, Šveices) informācijas drošības departamenta pārstāvis var tikt iecelts par kiberdrošības pārvaldnieku Latvijas uzņēmumā, taču ar nosacījumu, ka viņš ir oficiāli norīkots organizācijas vadītāja lēmumā, ir paziņots NKDC un spēj praktiski nodrošināt kiberdrošības pārvaldību Latvijā. Galvenais kritērijs nav pilsonība vai atrašanās vieta, bet gan juridiska atbildība un reāla pieejamība uzņēmuma darbības nodrošināšanai Latvijā (tostarp incidenta gadījumā).

19. Kādi ir ierobežojumi kiberdrošības pārvaldnieka iecelšanai (piemēram, kvalifikācijas vai drošības prasības)?

Kiberdrošības pārvaldniekam jāatbilst vairākiem kritērijiem, kas detalizēti ir noteikti MK noteikumu Nr. 397 3.1. apakšnodaļā. Aicinām iepazīties ar NKDC infografiku “Kas ir kiberdrošības pārvaldnieks?”: šeit.

20. Vai, piemēram, ministrijai un visām tās padotības iestādēm var tikt iecelts viens kiberdrošības pārvaldnieks?

Saskaņā ar MK noteikumu Nr. 397 19. punktu kiberdrošības pārvaldnieks drīkst strādāt arī iestādes (piem., ministrijas) padotības iestādēs bez skaita ierobežojuma, kamēr vien kāda no tām nav IKT KI īpašnieks vai tiesiskais valdītājs. Gadījumā, ja ministrija vai kāda tās padotības iestāde ir IKT KI īpašnieks vai tiesiskais valdītājs, lūdzu skatīt ierobežojumus atbildē uz 13. jautājumu. Piemērotība vienam kiberdrošības pārvaldniekam vairākām iestādēm jāvērtē, ņemot vērā IKT infrastruktūras centralizāciju un iespējamos riskus pret ieguvumiem.

21. Vai pašvaldības kapitālsabiedrībai, kas atzīta par būtisko pakalpojumu sniedzēju, ir jāieceļ kiberdrošības pārvaldnieks (saskaņā ar NKDL 25. pantu un MK noteikumiem Nr. 397, ja uzņēmuma īpašumā nav informācijas sistēmu un visas izmantotās sistēmas (piemēram, grāmatvedības, dokumentu aprites, e-pasta, luksoforu vadības un pilsētas apgaismojuma vadības sistēmas) ir ārpakalpojumu sniedzēju īpašumā un pārvaldīšanā? Kapitālsabiedrība ir tikai šo sistēmu lietotājs bez administratora tiesībām.

Skaidrojam, ka katra NKDL subjekta kompetencē ir izvērtēt piemērotākos kiberdrošības organizatoriskos un tehniskos pasākumus. Līdz ar to, attiecīgajam subjektam ir saistoši MK noteikumi Nr. 397, kas cita starpā paredz minimālās kiberdrošības prasības pasākumus, t.sk. kiberdrošības pārvaldnieka noteikšanu un rīcību kiberincidentu gadījumā. Vienlaikus vēršam uzmanību, ka kiberdrošības pārvaldība var tikt nodrošināta arī ārpakalpojuma ietvarā, pirms tam izvērtējot ar to saistītos iespējamos drošības un atbilstības riskus katrā konkrētajā gadījumā. Tāpat norādām, ka kiberdrošības pārvaldnieka kompetencē ietilpst uzdevumi, kas var nebūt tieši saistīti ar informācijas sistēmu pārvaldību, piemēram, subjekta sniegto pakalpojumu darbības nepārtrauktības nodrošināšana, incidentu risināšana un ziņošana. Pat ja visas subjekta informācijas sistēmas ir ārpakalpojumi, kiberdrošības pārvaldniekam tik un tā jānodrošina, ka darbinieki sistēmām piekļūst droši, ievēro kiberhigiēnas principus, ir apmācīti darbam ar tām.

APMĀCĪBAS

22. Vai sākotnējā instruktāža attieksies arī uz sētniekiem, apkopējām un citiem darbiniekiem, kas nestrādā ar informācijas sistēmām?

Kiberhigiēnas apmācības organizē nodarbinātajiem, kas strādā ar konkrētā uzņēmuma/iestādes informācijas sistēmām. Apmācības attiecas gan uz priviliģētajiem lietotājiem, gan citiem lietotājiem, kuri piekļūst, piemēram, e-pastam.

23. Vai tiks organizētas apmācības valsts un pašvaldību iestādēm?

NKDC regulāri organizē informatīvus seminārus NKDL subjektiem. CERT.LV divas reizes gadā organizē apmācības kiberdrošības pārvaldniekiem. Vienlaikus vēršam uzmanību uz to, ka Valsts administrācijas skolā ir pieejams bezmaksas kurss: Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem, lai sniegtu praktiskas zināšanas par kiberhigiēnas jautājumiem publiskās pārvaldes darbiniekiem, kā arī citi noderīgi kursi un kiberdrošības pārvaldības pilnveides darbnīcas.

24. Vai būs kāds seminārs par pašvērtējuma ziņojuma aizpildīšanu?

Par gaidāmajiem semināriem informācija tiks publicēta cyber.gov.lv mājaslapā. Iesakām iepazīties ar NKDC publicētajiem kiberdrošības pārvaldības dokumentācijas paraugiem un vadlīnijām: šeit. Papildus aicinām neskaidrību gadījumus par pašvērtējuma ziņojuma precīzu aizpildīšanu rakstīt uz NIS2@mod.gov.lv.

TEHNISKĀS PRASĪBAS

25. Vai varat sniegt kādus ieteikumus, kas palīdzētu labāk izprast, kā īstenot MK noteikumos Nr. 397 noteiktās prasības?

Cyber.gov.lv mājaslapā ir pieejami kiberdrošības pārvaldības dokumentācijas paraugi, kā arī ir publicētas kriptogrāfijas, informācijas sistēmu un resursu drošības klašu noteikšanas, rezerves kopiju veidošanas, žurnālfailu vadlīnijas: šeit.

26. Vai IS darbības nodrošināšanai drīkst izmantot atvērtā koda vai bezmaksas programmnodrošinājumu, kuru ir radījusi kopiena (fizisku personu grupa), kuru valstiskā piederība precīzi nav zināma?

Var, bet ir jāizvērtē potenciālie riski pret ieguvumiem. Atvērtā koda būtība – liels loks ar izstrādātājiem un entuziastiem – lielā mērā izslēdz iespēju vienam izstrādātājam/programmētājam kodā ietvert ļaunatūru. Vienlaikus, lai pārliecinātos par koda drošumu, vēlams veikt tā revīziju un pārskatīt atvērtā koda programmatūras konfigurāciju pēc lielāku atjauninājumu veikšanas.

Piegādātājs vai pat lietotājs, ja viņam ir nopietns nodoms balstīt savus risinājumus uz konkrēto atvērtā koda sistēmu vai bibliotēku, pats var kļūt par vienu no "entuziastiem", kas attīsta konkrēto atvērto kodu vai var veidot savu atzaru "branch", kuru attīsta un neļauj citiem "entuziastiem" tajā kaut ko pievienot.

Vienlaikus, IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam gadījumā, ja programmatūru ir plānots izmantot A klases informācijas sistēmā un subjekts nevar

pārliecināties par tās atbilstību MK noteikumu Nr. 397 94.punkta prasībām, pirms tās izmantošanas ir jāsaņem SAB atzinums (MK noteikumu Nr. 397 95. punkts).

27. KI turētāja A klases informācijas sistēma izvietota mākoņpakalpojuma resursos: a) vai šajā gadījumā mākoņpakalpojuma sniedzēja resursi ir uzskatāmi par kritisko infrastruktūru un b) vai mākoņpakalpojuma sniedzējam, piemēram, Microsoft, ir jānodrošina pašnovērtējuma u.c. ziņojumu sagatavošana?

Aicinām iepazīties ar MK noteikumu Nr. 397 iekļauto informācijas sistēmu gradāciju (5. pielikums), lai pārliecinātos, ka tiešām pārvaldāt A klases informācijas sistēmu jaunā regulējuma ietvarā. Jāņem vērā arī tas, ka A klases informācijas sistēmas var atrasties ne tikai IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja pārvaldībā.

Vēršam uzmanību, ka saistībā ar šo tiek izstrādāti citi noteikumi "Noteikumi par informācijas sistēmu izvietošanu un datu centru drošības prasībām". Tajos tiks noteikts kādos datu centros atļauts izvietot A drošības klases IS.

Pašvērtējuma sagatavošana jebkurā gadījumā ir subjekta, nevis ārpakalpojuma sniedzēja atbildība.

28. Vai informācijas sistēmas ar A drošības klasi var būt tikai būtisko pakalpojumu sniedzējam? Vai svarīgo pakalpojumu sniedzējiem informācijas sistēmu drošības klase pēc noklusējuma nevar būt augstāka par B drošības klasi?

Nē, A drošības klases informācijas sistēma var būt gan būtisko pakalpojumu sniedzēja, gan svarīgo pakalpojumu sniedzēja, gan IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja pārvaldībā.

29. Vai MK noteikumi Nr. 397 darbojas arī uz IKT pilotprojektiem, kas tiks darbināti KI vidē?

Noteikumi nosaka minimālās kiberdrošības prasības būtisko un svarīgo pakalpojumu sniedzējiem, kā arī IKT kritiskās infrastruktūras īpašniekiem un pārvaldītājiem. Tie attiecas uz jebkuru sistēmu vai projektu, kas tiek ieviests vai lietots KI, neatkarīgi no tā, vai tas ir pilotprojekts vai pilnvērtīga sistēma. KI un IKT KI infrastruktūras gadījumā jebkuras darbības tiek saskaņotas un vērtētas individuāli, iesaistot uzraugošās iestādes.

30. Kas saskaņā ar NKDL un MK noteikumiem Nr. 397 ir uzskatāmas par "valdījumā esošas informācijas un komunikācijas tehnoloģijas"? Kādas ir pazīmes pēc kurām jāvadās, lai noteiktu vai informācijas un komunikācijas tehnoloģijas (turpmāk – "IKT") ir subjekta valdījumā esošas?

Par valdījumā esošām IKT uzskatāmas:

- Iekārtas, sistēmas un tīkli, kas atrodas subjekta īpašumā vai valdījumā (vai pārvaldībā – ar iespējām noteikt procedūras, loģiskas kontroles, atbildības, fizisku piekļuvi u.tml.).

– Sistēmas, kurām subjektam ir administratīva kontrole (piem., serveri, darba stacijas, tīkla iekārtas – ar iespējām noteikt kontroli un konfigurāciju, sekot līdzi notikumiem un slēgt loģisku piekļuvi, u.tml.).

Pazīmes: piekļuves tiesības, konfigurācijas pārvaldība, atbildība par uzturēšanu un drošību.

Ja pakalpojums ir ārpakalpojumā (piem., mākonis), tad tas nav "valdījumā esošs", bet ir jāvērtē atbilstoši līgumam un drošības prasībām, kurām jābūt ekvivalentām MK noteikumu Nr. 397 prasībām.

31. Ja kritiskās infrastruktūras IT sistēmai tiek veidots rīks datu analizēšanai (piemēram, uz MS Fabric bāzes), vai datu noliktavai ar datiem obligāti jābūt bāzētiem Latvijā, vai var tikt izmantoti mākoņpakalpojumi, kas datus uzglabā Eiropas Savienības teritorijā?

Šajā gadījumā rīkam ir jāatbilst MK noteikumu Nr, 397 94. punkta noteiktajām prasībām. Jautājums ir jārisina individuāli un jāsaskaņo, iesaistot IKT KI uzraugošo iestādi, kā arī papildus vērtējama atbilstība ar personu datu aizsardzību saistītajam tiesību normu regulējumam, t.sk. nepieciešamības gadījumā konsultējoties Datu valsts inspekcijā.

PAR DROŠĪBAS KLASĒM

32. Saskaņā ar MK noteikumu Nr. 397 34. pantu: "Kritiskās infrastruktūras kopumā iekļautu informācijas sistēmu uzskata par A klases informācijas sistēmu, nepiemērojot šo noteikumu 32. un 33. punktā minēto kārtību." Ja sistēmas (piemēram, video novērošana, piekļuves punkti, apsardzes sistēmas) tiek uzskatītas par neatņemamu kritiskās infrastruktūras daļu, tās automātiski kvalificējas kā A klases informācijas sistēmas. Vai šādā gadījumā ir nepieciešams aizpildīt 5. pielikumu, kas paredzēts drošības klases izvērtēšanai?

Vēršam uzmanību uz MK noteikumu Nr. 397 35. punktā noteikto, proti, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Subjekta informācijas sistēmu drošības klases nosakāmas saskaņā ar MK noteikumu Nr. 397 5. pielikumā ietverto metodiku. Ņemot vērā norādīto, subjektam nepieciešams noteikt konfidencialitātes, integritātes un pieejamības drošības klasi (A, B vai C) katrai subjekta īpašumā un valdījumā esošajai informācijas sistēmai un informācijas resursu kategorijai, un saskaņā ar MK noteikumu Nr. 397 35. punktā noteikto, nosūtīt tās saskaņošanai SAB.

33. A klases IS, kas nav kritiskā, SAB atzinumu neprasa, tikai izvērtē atbilstoši 101. p. (94. p.)?

Skaidrojam, ja IS īpašnieks ir IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs un, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Savukārt saskaņā ar MK noteikumu Nr. 397 101. punktā noteikto, būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, ārpakalpojuma līgumu A klases informācijas sistēmai atļauts slēgt, ja ārpakalpojuma sniedzējs tehniskā

resursa iegādei un tehniskā resursa ražotājs atbilst šo noteikumu 94. punktā noteiktajām prasībām.

34. Vai sanāk, ka subjektam, kurš ir iekļauts IKT KI, neatkarīgi no kategorijas, visas IS pēc noklusējuma ir A klases IS, līdz brīdim kad ar SAB saskaņo citus, zemākus līmeņus?

Skaidrojam, ja IS īpašnieks ir IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs un, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Savukārt saskaņā ar MK noteikumu Nr. 397 101. punktā noteikto, būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, ārpakalpojuma līgumu A klases informācijas sistēmai atļauts slēgt, ja ārpakalpojuma sniedzējs tehniskā resursa iegādei un tehniskā resursa ražotājs atbilst šo noteikumu 94. punktā noteiktajām prasībām.

35. Cik saprotu, tad 94. punkts noteikti attiektos uz servera iegādi, uz kura tiktu uzlikta A klases sistēma. Jautājums vai 94. punkts attieksies uz tīkla iekārtām, kas nodrošinās piekļuvi serverim?

MK noteikumu 94. punkts attiecas uz tīkla iekārtām un citiem IKT resursiem, kas nodrošinās piekļuvi serverim, ja tīkla iekārta ir A klases sistēmas sastāvdaļa vai ietekmē A klases sistēmas darbību (piemēram, nodrošinot piekļuvi serverim, nodrošina datu plūsmu u.c.) vai tā var ietekmēt A klases sistēmas drošību (piemēram, uzlaužot tīkla iekārtu, var iegūt piekļuvi A klases sistēmas serverim vai datiem) vai tā ir daļa no infrastruktūras, kurā tiek izvietota attiecīgā A klases sistēma

36. Ja DELL (ASV) dators ražots Ķīnā un piegādātājs ir kompānija Latvijā, tad iekārta ir atbilstoša?

MK noteikumu Nr. 397 86.5. apakšpunkts nosaka, ka subjekts ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi nedrīkst slēgt, ja iegādājamā IKT resursa ražotājs ir šo noteikumu 86.1. apakšpunktā minētajā valstī reģistrēta juridiska persona vai šīs valsts pilsonis (Vispārīgās ārpakalpojumu prasības). Šo noteikumu 94. punkts savukārt nosaka, ka IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi atļauts slēgt, ja ārpakalpojuma sniedzējs un tehniskā resursa ražotājs atbilst 94. punktā ietvertajiem kritērijiem.

Savukārt, noteikumu 101.1. apakšpunkts nosaka, ka būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, ārpakalpojuma līgumu A klases informācijas sistēmai atļauts slēgt, ja ārpakalpojuma sniedzējs tehniskā resursa iegādei un tehniskā resursa ražotājs atbilst šo noteikumu 94. punktā noteiktajām prasībām.

Ņemot vērā norādīto, ir jāvērtē valsts, kurā IKT resurss tiek ražots.

37. Ja vienā IKT resursā atrodas A sistēma un C sistēma, vai C sistēmai arī ir A sistēmas drošības prasības?

Jā, ja C klase fiziski atrodas uz tā paša resursa, kas apkalpo A klasi, tad jānodrošina A klases prasību izpilde visam resursam, lai neradītu drošības riskus. Tas izriet no 94. punkta un

vispārīgajām drošības prasībām. Vienlaikus, C drošības klases informācijas sistēmai nav jāpiemēro A drošības klases informācijas sistēmai noteiktās drošības prasības.

38. Ja A no SAB saņem atļauju sadarboties ar B. Vēlāk C no SAB saņem aizliegumu sadarboties ar B. Vai A saņems info no SAB, ka ir problēmas ar B (jālauž līgums, citas darbības)?

Skaidrojam, ka SAB var informēt subjektus par nepieciešamību izvērtēt sadarbību ar attiecīgu komersantu, vienlaikus komersanta un ārpakalpojuma izpildei piesaistītu citu pakalpojuma sniedzēju pārbaude tiek veikta, sniedzot SAB atzinumu MK noteikumu Nr. 397 noteiktajā kārtībā.

39. Kritiskajā objektā atrodas sistēmas serveris un daļa aprīkojuma, kas ir klasificēti kā A klase. Vai ir pareizi uzskatīt, ka arī pārējās šīs sistēmas iekārtas, kas atrodas citos reģionos un kalpo kā datu pārsūtītāji, automātiski jāuzskata par A klases iekārtām?

Skaidrojam, ka objektam (piemēram, ēka, inženierbūve u.c.) noteiktajam KI objekta statusam nav korelācijas ar tajā esošajiem resursiem piešķirtajām drošības klasēm.

Vēršam uzmanību, ka Ministru kabineta 2026. gada 13. janvāra noteikumi Nr. 10 "Kritiskās infrastruktūras apzināšanas, darbības nepārtrauktības, drošības un noturības pasākumu plānošanas, īstenošanas un incidentu paziņošanas kārtība" (turpmāk - MK noteikumi Nr. 10) nosaka, ka valsts drošības iestādes apzina iespējamo A, B un C kategorijas kritisko infrastruktūru un šie noteikumi nenosaka informācijas sistēmas konfidencialitātes, integritātes un pieejamības drošības klases. MK noteikumos Nr. 10 ietvertā kritiskās infrastruktūras klasifikācija izriet no Nacionālās drošības likuma 22.2. panta otrajā daļā ietvertās klasifikācijas.

Skaidrojam, ka, piemēram, gadījumā, ja MK noteikumu Nr. 10 izpratnē tiek piešķirta B kategorijas kritiskās infrastruktūras statuss, tas nenozīmē, ka visām sistēmām MK noteikumu Nr. 397 izpratnē arī tiks piešķirta B drošības klase.

40. Kritiskajā objektā atrodas sistēmas serveris un daļa aprīkojuma, kas ir klasificēti kā B klase. Vai šo sistēmu uzskata kā kritiskās infrastruktūras kopumā esošu sistēmu un jāpārvērtē kā A sistēmu?

Skaidrojam, ka objektam (piemēram, ēka, inženierbūve u.c.) noteiktajam KI objekta statusam nav korelācijas ar tajā esošajiem resursiem piešķirtajām drošības klasēm.

Skaidrojam, ka saskaņā ar jaunajos MK noteikumos Nr. 397 noteikto un augstāk minēto, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Vienlaikus norādām, ka KI objektā var būt informācijas sistēmas, kas ir zemākas klases par A drošības klasi.

41. Ja mūsu kritiskajā objektā atrodas datu pārraides tīkls, kas nodrošina sistēmas darbību, vai šis tīkls ir automātiski jāuzskata par A klases informācijas sistēmu? Papildus tam, ja par šo datu pārraides tīklu ir atbildīga cita iestāde, vai mēs kā kritiskās infrastruktūras subjekts esam atbildīgi par to, lai informētu šo iestādi par tīkla klasificēšanu kā A klases sistēmu un nodrošinātu atbilstību mūsu prasībām?

Skaidrojam, ka objektam (piemēram, ēka, inženierbūve u.c.) noteiktajam KI objekta statusam nav korelācijas ar tajā esošajiem resursiem piešķirtajām drošības klasēm.

Gadījumā, ja kritiskajā objektā atrodas datu pārraides tīkls, kas nodrošina sistēmas darbību, vai šis tīkls ir automātiski jāuzskata par A klases informācijas sistēmu, vēršam uzmanību uz to, ka datu pārraides tīkls nodrošina informācijas sistēmas darbību, tas parasti tiek uzskatīts par šīs informācijas sistēmas būtisku sastāvdaļu, bet ne obligāti par atsevišķu informācijas sistēmu. Vienlaikus gadījumā, ja šis datu pārraides tīkls nodrošina A klases informācijas sistēmas darbu, tas būtu klasificējams kā A klases informācijas sistēmas sastāvdaļa.

42. Gadījumā, ja mēs kā iestāde esam noteikti par B klases kritisko infrastruktūru, tajā esošās informācijas sistēmas saskaņā ar MK noteikumu Nr. 397 34. pantu, automātiski jāuzskata par A klases sistēmām?"

Saskaņā ar MK noteikumiem Nr. 397 35. punktā noteikto, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB, nosakot konfidencialitātes, integritātes un pieejamības drošības klasi (A, B vai C) atbilstoši šo noteikumu 5. pielikumā ietvertajai metodikai katrai subjekta īpašumā un valdījumā esošajai informācijas sistēmai un informācijas resursu kategorijai.

INFORMĀCIJAS IESNIEGŠANA NKDC

43. Kad uzņēmumam jāiesūta sākotnējā informācija, konstatējot, ka tas atbilst NKDL subjekta statusam?

Subjekta statusa atbilstības paziņojuma iesniegšanas termiņš ir viens mēnesis pēc atbilstības iestāšanās.

Savukārt līdz attiecīgā kalendārā gada 1. oktobrim NKDL subjektiem jāiesniedz pašvērtējuma ziņojums un jāinformē par kiberdrošības pārvaldnieka iecelšanu.

Ja atbilstība subjekta statusam ir iestājusies pēc 1. jūlija, subjekts pirmreizējo pašvērtējuma ziņojumu iesniedz ne vēlāk kā triju mēnešu laikā no atbilstības brīža.

44. Kā noformēt iesniedzamo informāciju? Vai ir pieejami šabloni?

Veidlapas (gan būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapa, gan domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusa paziņojuma veidlapa, gan paziņojuma par kiberdrošības pārvaldnieka nozīmēšanu veidlapa) pieejamas MK noteikumu Nr. 397 esošajos pielikumos.

45. Kā nosūta informāciju NKDC?

Izmantojot Latvija.lv, nosūta ziņojumu un elektroniski parakstītas veidlapas uz Aizsardzības ministrijas Nacionālā kiberdrošības centra oficiālo e-adresi (NKDC@90000022632).

46. Kā informēt NKDC un SAB par kiberdrošības pārvaldnieka iecelšanu?

Saskaņā ar NKDL 25. panta otrajā daļā noteikto par kiberdrošības pārvaldnieka noteikšanu ir jāziņo gan NKDC, gan SAB nekavējoties, bet ne vēlāk kā piecu darbdienu laikā. Jāņem vērā, ka IKT KI īpašniekam kiberdrošības pārvaldnieka iecelšana pirms tam jāsaskaņo ar SAB, un tam ir noteikta atsevišķa veidlapa MK noteikumu Nr. 397 pielikumā.

Veidlapa par kiberdrošības pārvaldnieka noteikšanu subjektā nosūtāma uz NKDC un SAB oficiālajām e-adresēm, atbilstoši NKDL noteiktajam subjektu uzraudzības dalījumam.

47. Ziņošana par incidentiem. Vai ir jāziņo par ikdienas mazsvarīgiem incidentiem?

Par kiberincidentiem, kuri nav uzskatāmi par nozīmīgiem kibernicidentiem atbilstoši MK noteikumu Nr. 397 118. punktā noteiktajam (piem., viena lietotāja paroles bloķēšana, neliels pikšķerēšanas mēģinājums, kas nav guvis panākumus), nav jāziņo CERT.LV, bet tie ir jāreģistrē organizācijas iekšējā incidentu pārvaldības sistēmā un/vai incidentu žurnālā. Savukārt par nozīmīgu kiberincidentu nekavējoties informē kompetento kiberincidentu novēršanas institūciju un izpilda tās sniegtos norādījumus par turpmāko rīcību incidenta pārvaldībā. Institūcijas informēšana norit saskaņā ar MK noteikumi Nr. 397, iesniedzot agrīno brīdinājumu (24 stundu laikā pēc incidenta konstatēšanas), sākotnējo ziņojumu (72 stundu laikā pēc incidenta konstatēšanas, bet uzticamības pakalpojumu sniedzējiem – 24 stundu laikā), kā arī gala ziņojumu (mēneša laikā pēc sākotnējā ziņojuma iesniegšanas). Ja mēneša laikā incidentu nav izdevies novērst, tiek iesniegts progresa ziņojums, bet pēc incidenta atrisināšanas iesniedzams gala ziņojums.

CITI JAUTĀJUMI

48. Kādi kiberdrošības risku pārvaldības pasākumi ir jāievēro digitālās infrastruktūras pakalpojumu sniedzējiem?

Pamatojoties uz NIS2 direktīvu ir izdota Eiropas Komisijas 2024. gada 17. oktobra *īstenošanas regula (ES) 2024/2690, kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka NIS2 Direktīvas piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku.*

Ar Īstenošanas regulā noteiktajām prasībām aicinām iepazīties: šeit. Norādām, ka īstenošanas regulas ir tieši piemērojamas un netiek pārņemtas nacionālajos tiesību aktos. Līdz ar to digitālās infrastruktūras pakalpojumu sniedzējiem primāri saistošas ir Īstenošanas regulas prasības, ja vien nacionālie tiesību akti neparedz citas papildu prasības, kas nepārklājas ar Īstenošanas regulā ietvertajām.

Vienlaikus jāņem vērā, ka digitālās infrastruktūras pakalpojumu sniedzēji var sniegt savus pakalpojumus citiem NDKL subjektiem, un šādā gadījumā tiem ir saistošas MK noteikumos Nr. 397 ietvertās ārpakalpojumu prasības.

49. Kāds ir NKDL ietverto subjektu uzraudzības sadalījums?

Atbilstoši NKDL 41. pantā noteiktajam, NKDL subjektu uzraudzību veic NKDC attiecībā uz būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, izņemot informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru. SAB veic uzraudzību attiecībā uz informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru.

Uzraudzību pār daļu subjektu veic arī Latvijas Banka un Civilās aviācijas aģentūra savas nozares ietvaros.

50. Kā interpretējams NKDL 20. panta 11. punkts?

NKDL 20. panta pirmās daļas 11. punkts ir iekļauts likumā, pamatojoties uz NIS2 direktīvas 2. panta 2. punkta d) apakšpunktu. Tas paredz, ka direktīvas I vai II pielikumā minētajām vienībām prasības piemēro neatkarīgi no to lieluma, ja to sniegtā pakalpojuma traucējums var radīt būtisku sistēmisku risku, īpaši nozarēs, kur šādam traucējumam var būt pārrobežu ietekme. Būtisks sistēmisks risks NIS2 direktīvas kontekstā attiecas uz situācijām, kad organizācijas vai pakalpojuma sniedzēja darbības traucējumi var radīt plašas un nopietnas sekas ne tikai attiecīgajā nozarē, bet arī citās nozarēs vai valstīs. Šāds risks var ietekmēt kritiskās infrastruktūras darbību, sabiedrības drošību, ekonomiku un vispārējo stabilitāti. Piemēram, ja traucējumi kādā nozares pakalpojumā, piemēram, enerģētikā, var novest pie plašiem elektrības padeves pārtraukumiem, tas var ietekmēt ne tikai enerģijas patērētājus, bet arī citas nozares, piemēram, transportu, veselības aprūpi un ražošanu. Tādējādi jau NIS2 direktīva uzsver nepieciešamību nodrošināt drošību un noturību pret šādiem traucējumiem, īpaši nozarēs, kurām ir potenciāls radīt pārrobežu ietekmi.

NKDL 20. panta 11. punkts ir tieši saistīts ar NIS2 direktīvas izpratni par būtisku sistēmisku risku. Gan NIS2 direktīvā, gan NKDL tiek uzsvērta nepieciešamība identificēt un aizsargāt būtiskos pakalpojumu sniedzējus, kuru darbības traucējumi var radīt nopietnas sekas sabiedrībai un valstij. NKDL 20. panta 11. punkts skaidri norāda, ka būtisko pakalpojumu sniedzēja darbības traucējumi var ietekmēt sabiedrības drošību, valsts aizsardzību un sabiedrības veselību, kā arī radīt būtisku sistēmisku risku, īpaši nozarēs ar potenciālu pārrobežu ietekmi. Tādējādi, gan NIS2 direktīva, gan NKDL uzsver nepieciešamību nodrošināt drošību un noturību pret traucējumiem, kas var ietekmēt plašāku sabiedrību un ekonomiku.

51. Ņemot vērā, ka pašvaldība atbilst būtisko pakalpojumu sniedzēja statusam, vai ir nepieciešams vērtēt katru pašvaldības iestādi atsevišķi saskaņā ar 20. panta 10. punktu?

Par katru NKDL atbilstošo juridisko personu nepieciešams iesūtīt savu statusa paziņojuma veidlapu. Pašvaldībai, vērtējot savas iestādes ir jāņem vērā to juridiskais statuss. Visbiežāk tās ir pastarpinātās pārvaldes iestādes (NKDL 20. panta 5. un 10. punkts).

52. Kā rīkoties situācijās, ja ir aizdomas, ka bibliotēkas apmeklētājs ir nonācis krāpnieku shēmās, bet pats to neizprot un nesaprot?

Bibliotēkās, ja apmeklētājs nonācis krāpnieku shēmās, darbiniekiem jāinformē par riskiem, jāsniedz apmeklētājam uzticami resursi un, ja nepieciešams, jāiesaista policija vai CERT.LV (e-pasta adrese - cert@cert.lv), ziņojot par konkrēto situāciju.

Neatradi atbildi uz interesējošo jautājumu? Raksti uz NIS2@mod.gov.lv