Nacionālais kiberdrošības centrs

https://cyber.gov.lv, NIS2@mod.gov.lv, 67335131

Informācijas sistēmas un resursu drošības klašu noteikšanas vadlīnijas

Saskaņā ar Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 38. punktu

Šīs vadlīnijas izstrādātas, lai palīdzētu Nacionālās kiberdrošības likuma subjektiem (būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem) noteikt savu IKT resursu un informācijas un to sistēmu drošības klases.

Versija 1.2, 17.03.2026

SATURS

1. IEVADS

1.1. MĒRĶIS UN PIEMĒROŠANAS JOMA

Šo vadlīniju mērķis ir nodrošināt vienotu pieeju informācijas un komunikācijas tehnoloģiju (IKT) resursu, informācijas un to sistēmu drošības klašu noteikšanai, kas ir būtiska daļa no kiberdrošības pārvaldības procesa.

Vadlīnijas piedāvā metodiku, kuru var piemērot visi Nacionālās kiberdrošības likuma (NKDL) subjekti, lai klasificētu informācijas sistēmas atbilstoši to konfidencialitātes, integritātes un pieejamības zuduma riskam un nodrošinātu atbilstību Eiropas Savienības NIS2 direktīvas (Direktīva (ES) 2022/2555) prasībām par vienādi augsta kiberdrošības līmeņa sasniegšanu visā Eiropas Savienībā.

1.2. NORMATĪVAIS KONTEKSTS

Vadlīnijas balstītas uz vairākiem normatīvajiem dokumentiem, kas kopumā veido tiesisko ietvaru kiberdrošības pārvaldībai Latvijā un Eiropas Savienībā:

NIS2 direktīva (Direktīva (ES) 2022/2555) – paredz pasākumus vienādi augsta kiberdrošības līmeņa nodrošināšanai visā ES, nosakot stingrākas prasības būtisko un svarīgo pakalpojumu sniedzējiem, tostarp risku pārvaldības pasākumus, incidentu ziņošanas kārtību un atbildības mehānismus.

Īstenošanas regula (ES) 2024/2690 – precizē NIS2 direktīvas piemērošanas noteikumus, nosakot:

- prasības attiecībā uz DNS pakalpojumu sniedzējiem, TLD reģistriem, mākoņdatošanas un datu centru pakalpojumu sniedzējiem, satura piegādes tīkliem, pārvaldītu pakalpojumu un drošības pakalpojumu sniedzējiem, tiešsaistes platformām un uzticamības pakalpojumu sniedzējiem;
- kritērijus, pēc kuriem incidents tiek uzskatīts par būtisku.

Ministru kabineta 2025. gada 25. jūnija noteikumi Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk - MK 397) nosaka metodiku būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem informācijas sistēmu drošības klašu piešķiršanai, balstoties uz trim riska dimensijām - konfidencialitāti, integritāti un pieejamību. Katram resursam vai sistēmai tiek piešķirta A, B vai C klase atbilstoši noteiktiem kritērijiem un pazīmēm. Tehniskiem resursiem klase tiek piešķirta, pamatojoties kiberdrošības riskam pakļautas informācijas sistēmas, kuram tas pieder.

2. TERMINI UN DEFINĪCIJAS[1]

Termins	Apraksts
Informācijas resurss	Strukturēts digitālo datu kopums, kas tiek elektroniski apstrādāts informācijas sistēmā (piem., datubāzes, dokumentu krājumi, reģistru ieraksti). Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam.
IKT resursi	Tehnisko resursu un informācijas resursu kopums. Piemēram: Serveri, datortīkli, ugunsmūri, datu glabāšanas iekārtas, darba stacijas, tīkla aktīvie elementi utt. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam.
Tehniskais resurss	Aparatūra, iekārta, kas ir tīkla vai informācijas sistēmas sastāvdaļa vai IKT infrastruktūrā izmantota iekārta, kas veic datu apmaiņu ar informācijas sistēmu, un programmatūra, tostarp operētājsistēmas, sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase nav tieši piemērojama, bet, ja uzskaite ir būtiska, tad tā piešķirama no informācijas sistēmas drošības klases.
Resursu kategorija	Resursu kategoriju piemēri nav tieši definēti MK 397, taču tās saprot kā informācijas veidus vai kā grupu ar līdzīgu aizsardzības līmeni.

[1] https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas#p2 Ministru kabineta noteikumos Nr. 397 lietotie termini

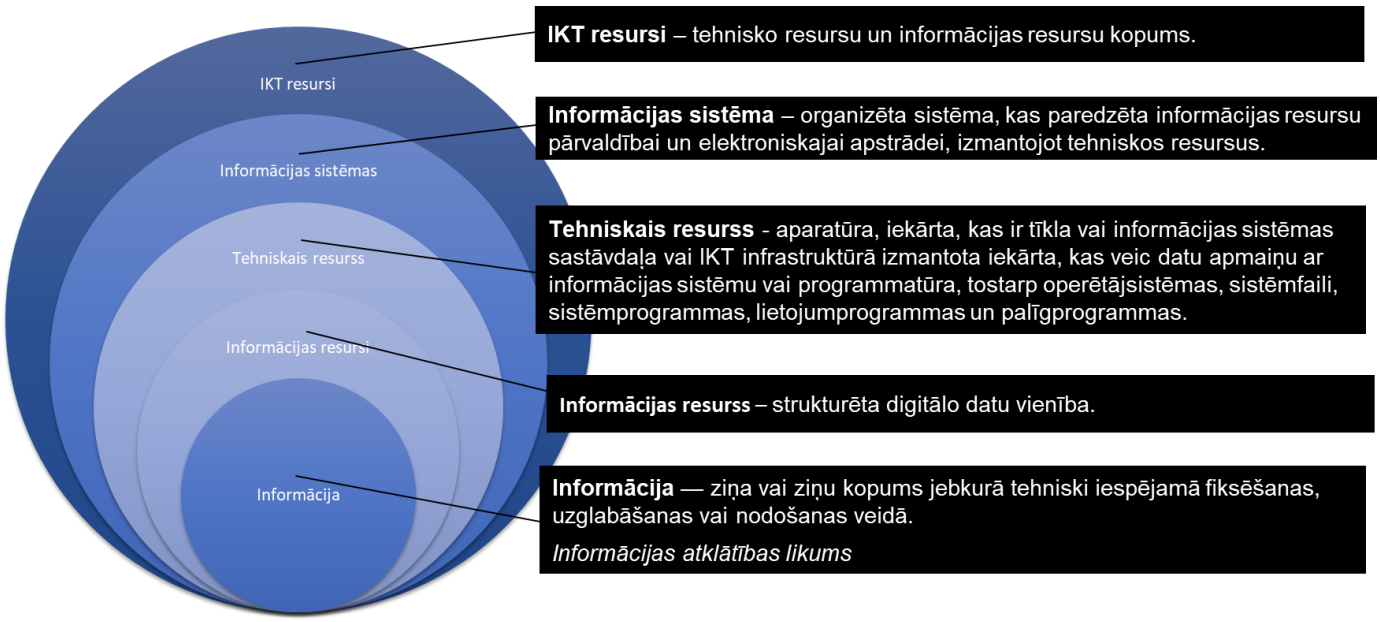
Informācijas sistēma	Organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam. Informācijas sistēmu drošības klašu noteikšana nosaka piemērojamo kiberdrošības prasību apjomu un stingrību. Sistēmas kategorija nosaka, kāds minimālais drošības pasākumu līmenis ir jāievieš, t. sk. tehnisko un organizatorisko un administratīvo kontroļu detalizācijas pakāpi, incidentu pārvaldības kārtību un atbilstības nodrošināšanas mehānismus. Zemākā piešķiramā klase kiberdrošības riskam pakļautam IKT resursam, informācijas sistēmai vai informācijai ir C (minimālās drošības).
Drošības pasākumi	Tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina risku līdz pieņemamam līmenim.
Drošības klase	IKT resursu un informācijas sistēmu kataloga informācijas resursa/sistēmas kritiskuma (ietekme uz valstiskiem procesiem, atbilstoši MK 397 5. pielikumam) pakāpe konfidencialitātes, integritātes un pieejamības riska dimensijās: klasēs A (augsta), B (vidēja), C (zema). Piezīme: noteikumos nav tieši aprakstīts drošības klases termins, taču ir aprakstīta noteikšanas metodika.
Ārpakalpojums	Jebkura veida vienošanās starp subjektu un pakalpojuma sniedzēju IKT jomā, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu, veic tehnisko resursu piegādi vai veic citu darbību subjekta uzdevumā IKT infrastruktūrā.

IKT resurss = "kopums" (tehnoloģija + dati).

Informācijas sistēma = Organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus.

Informācijas resurss = Strukturēts digitālo datu kopums, kas tiek elektroniski apstrādāts informācijas sistēmā (piem., datubāzes, dokumentu krājumi, reģistru ieraksti).

Tehniskais resurss = "lietojumprogramma, operētājsistēma" – tas ir viss, ar ko tiek nodrošināta datu ievade, apstrāde, pārraide vai glabāšana. Atšķirībā no **informācijas resursa** (dati, saturs), tehniskais resurss ir vide, kurā šie dati atrodas un ar kuru tie tiek apstrādāti.



3. DROŠĪBAS KLAŠU NOTEIKŠANAS METODIKA (MK 397, 5. PIELIKUMS)

3.1. VISPĀRĪGIE PRINCIPI

Katrai drošības riska dimensijai (konfidencialitāte, integritāte, pieejamība) piešķir atsevišķu klasi (A/B/C), balstoties uz noteiktiem kritērijiem. Klasifikāciju dokumentē un uztur aktuālu.

A drošības klasi piešķir, ja attiecīgās informācijas sistēmas vai datu integritātes, pieejamības un konfidencialitātes pārkāpums varētu radīt ļoti nopietnas sekas sabiedrībai vai valstij.

B drošības klasi piešķir, **ja** datu noplūde (piemēram, "ierobežotas pieejamības" informācijas noplūde), sagrozīšana vai nepieejamība sistēmā var būtiski ietekmēt pašas organizācijas darbību vai sniegtos pakalpojumus, bet nerada tūlītēju valsts mēroga apdraudējumu.

C drošības klasi piešķir, ja datu pieejamība, kļūdas vai izmaiņas nebūtiski ietekmē pamatdarbību.

Praktisks ieteikums: Klasificē pēc visjutīgākā sistēmā esošā resursa (ja sistēmā ir A drošības klases informācija, sistēmu no konfidencialitātes viedokļa vērtē kā A).

3.2. KONFIDENCIALITĀTE

A klase (augsta ietekme valsts pamatfunkciju īstenošanai)
— ļoti lieli personas datu apjomi (piem., ≥1 000 000 datu subjektu);
— īpašo kategoriju vai personas dati ļoti lielā apjomā (piem., ≥500 000);
— Informācija, kuras izpaušana kaitētu nacionālajai drošībai.
B klase (vidēja ietekme valsts pamatfunkciju īstenošanai)

— “Ierobežotas pieejamības informācija”;
— ≥5 000 īpašas kategorijas personas datu;
— noplūde rada būtisku reputācijas risku valstij/iestādei.
C klase (zema ietekme valsts pamatfunkciju īstenošanai)
— noplūde neradītu būtisku kaitējumu (piem., publiski dati);
— minimālās aizsardzības prasības saglabājas.

3.3. INTEGRITĀTE

A klase (augsta ietekme valsts pamatfunkciju īstenošanai)
— integritātes pārkāpums var pārtraukt vai būtiski traucēt valsts/pašvaldības pamatfunkcijas vai kritisko infrastruktūru;
— iespējamas katastrofālas sekas.
B klase (vidēja ietekme valsts pamatfunkciju īstenošanai)
— būtiski traucē subjekta darbību vai būtiskā/svarīgā pakalpojuma sniegšanu;
— iespējama sektoriāla ietekme uz citiem subjektiem (var apgrūtināt darbību citām IS).
C klase (zema ietekme valsts pamatfunkciju īstenošanai)
— integritātes kļūdas rada nelielas, viegli labojamas sekas;
— pamatfunkcijas netiek būtiski ietekmētas.

3.4. PIEEJAMĪBA

A klase (augsta ietekme valsts pamatfunkciju īstenošanai)
— neplānots dīkstāves laiks ≤0,1% mēnesī (~≤45 min/mēn.);
— un/vai ietekme uz pamatfunkcijām vai arī no sistēmas atkarīgas A drošības klases sistēmas.
B klase (vidēja ietekme valsts pamatfunkciju īstenošanai)
— neplānots dīkstāves laiks ≤1% mēnesī (~≤7 h /mēn.);
— būtiska ietekme uz subjekta pakalpojumu sniegšanu;
— atkarīgas B drošības klases sistēmas.
C klase (zema ietekme valsts pamatfunkciju īstenošanai)
— Pieļaujama dīkstāve >1% mēnesī, ja netiek būtiski ietekmētas pamatfunkcijas.

3.5. KOPĒJĀS KATEGORIJAS NOTEIKŠANA

Informācijas sistēmas drošības klase sakrīt ar augstāko riska līmeņa konfidencialitātes, integritātes un pieejamības (angļu val.: *Confidentiality, Integrity, Availability* jeb CIA) riska līmeņa dimensiju.

MK 397 33. punkts nosaka kā sistēma tiek klasificēta kopumā (A, B vai C klase) atkarībā no piešķirtajām klasēm konfidencialitātes, integritātes un pieejamības aspektos:

- **33.1.** **A** drošības klases **(paaugstinātas drošības)** informācijas sistēmu, ja tai ir noteikta vismaz viena A konfidencialitātes, integritātes vai pieejamības drošības klase;
- **33.2.** **B** drošības klases **(pamata drošības)** informācijas sistēmu, ja tai ir noteikta vismaz viena B konfidencialitātes, integritātes vai pieejamības drošības klase, bet nav noteikta neviena A konfidencialitātes, integritātes vai pieejamības drošības klase;
- **33.3.** **C** drošības klases **(minimālās drošības)** informācijas sistēmu, ja tai ir noteiktas tikai C konfidencialitātes, integritātes un pieejamības drošības klases.

Drošības klasēm atšķiras daudzfaktoru autentifikācija (angļu val.: *Multi-Factor Authentication* jeb MFA), žurnālfailu, rezerves kopiju, ārpakalpojumu u.c. prasības (paaugstinātas drošības sistēmām – augstākas).

Šāda kategorizācija ir būtiska, jo MK 397 daudzviet nosaka **atšķirīgas prasības A un B drošības klases sistēmām, salīdzinot ar C drošības klases sistēmām**.

Piemēram:

- **Autentifikācija un piekļuve:** A drošības klases sistēmās obligāti jānodrošina daudzfaktoru autentifikācija gan administratoriem, gan lietotājiem, savukārt B drošības klases – vismaz administratīvajiem kontiem. C drošības klases sistēmām šāda prasība var nebūt tieši noteikta (tomēr joprojām ieteicama pēc riska izvērtējuma).
- **Žurnālfailu glabāšana:** MK 397 paredz, ka žurnālfaili (log faili) A drošības klases sistēmās jāglabā vismaz 18 mēnešus, B drošības klases – 12 mēnešus, bet C drošības klases sistēmām šajā kontekstā var pietikt ar 6 mēnešiem.
- **Rezerves kopijas:** Paaugstinātas drošības sistēmām (A klases) ir stingrāki backup režīmi – piemēram, A drošības klases sistēmas rezerves kopiju uzglabāšanai jābūt ģeogrāfiski atdalītā vietā un īpaši aizsargātās telpās u.c. B drošības klases – arī jāievēro vairāku kopiju princips, bet var būt nedaudz mazāk striktas prasības. C drošības klases sistēmām pietiek ar pamatprasībām.
- **Ārpakalpojumu izmantošana:** Ārpakalpojumu (piemēram, mākoņpakalpojumu) izmantošana A drošības klases sistēmām ir ierobežota. B un C drošības klases sistēmām attiecīgi šie ierobežojumi ir mazāk strikti. IKT KI īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A drošības klases informācijas sistēmai atļauts slēgt tikai pēc SAB atzinuma saņemšanas.

Aizlieguma nosacījums	Apraksts
Aizliegtas valsts juridiska persona	Nedrīkst slēgt līgumu ar juridisku personu, kas reģistrēta Krievijā, Baltkrievijā vai valstī, ko Eiropas Parlaments vai Latvijas Republikas Saeima atzinusi par terorismu atbalstošu.
Aizliegtas valsts pilsonis	Nedrīkst slēgt līgumu, ja sniedzējs, tā dalībnieks, kapitāldaļu īpašnieks vai patiesais labuma guvējs ir noteikumu 86.1. apakšpunktā minētās valsts pilsonis.
Valdes vai padomes sastāvs	Nedrīkst slēgt līgumu, ja valde vai padome sastāv no fiziskām personām, kas ir noteikumu 86.1. apakšpunktā minētās valsts pilsoņi.
Iesaistītas personas pakalpojuma sniegšanā	Nedrīkst slēgt līgumu, ja pakalpojuma sniegšanā iesaistīts noteikumu 86.1. apakšpunktā minētās valsts pilsonis.
IKT resursa ražotāja izcelsme	Nedrīkst iegādāties IKT resursu, ja ražotājs ir juridiska persona, kas reģistrēta noteikumu 86.1. apakšpunktā minētajā valstī, vai šīs valsts pilsonis.

3.6. UZRAUDZĪBA

Nacionālais kiberdrošības centrs (NKDC) nodrošina Nacionālās kiberdrošības likuma (NKDL) subjektu uzraudzību un koordinēšanu. Tā darbības joma aptver gan publisko, gan privāto sektoru, atbilstoši Nacionālās kiberdrošības likuma 20. un 21. pantā noteiktajam subjektu lokam.

Satversmes aizsardzības birojs (SAB) ir atbildīgs par informācijas un komunikācijas tehnoloģiju (IKT) kritiskās infrastruktūras uzraudzību un tās aizsardzību pret draudiem nacionālajai drošībai. SAB kompetencē ietilpst informācijas komunikāciju tehnoloģiju kritiskās infrastruktūras objekti.

Sektora regulatori veic nozares specifisko prasību uzraudzību, pamatojoties uz attiecīgajiem normatīvajiem aktiem. To atbildība attiecas uz konkrētām nozarēm, piemēram, finanšu, veselības, transporta un enerģētikas sektoriem.

5. PRAKTISKIE PIEMĒRI

5.1. DROŠĪBAS KLAŠU PIEMĒROŠANA

<u>Piemērs 1:</u> Publiska informācijas vietne (portāls).

Valsts iestādes publisku tīmekļa portālu, kur iedzīvotāji var lasīt jaunākās ziņas, piekļūt publiskiem dokumentiem un instrukcijām.

Konfidencialitātes drošības klase: Šādā vietnē **nav konfidenciālas informācijas** – viss saturs ir paredzēts publiskai piekļuvei. Tātad informācijas resursa **konfidencialitātes klase būtu C**, jo noplūde (faktiski vietne jau ir atklāta) neradītu kaitējumu.

Integritātes drošības klase - ja kāds ļaunprātīgi izmainītu vietnes saturu (piemēram, aizstātu tekstus), tas varētu kaitēt iestādes reputācijai, bet **nekavētu pamatfunkciju izpildi** – iestādes iekšējās kontroles (pieņemsim, atļauju izsniegšana vai pakalpojumi) netiek veiktas caur šo vietni. Tātad integritātes pārkāpums būtiski neietekmē ne iestādes, ne citu subjektu darbu, klasificējam **C integritāti**.

Pieejamības drošības klase: portāla nepieejamība pāris stundu vai pat dienas garumā ir nepatīkama, bet nerada tiešas krīzes – iedzīvotājiem nebūtu piekļuves pie informācijas, ko var iegūt citur vai vēlāk. Tādēļ arī **pieejamību var klasificēt kā C**, ja iestāde var atļauties vairāk nekā 1% dīkstāvi mēnesī. Kopumā šī **informācijas sistēma būtu C drošības klases sistēma** (pamata drošības sistēma).

C/C/C – pamata drošība (pietiek ar pamata kontrolēm, atjauninājumiem un monitoringu). Informācijas sistēmas kopējā klase ir C.

<u>Piemērs 2:</u> Privāta uzņēmuma iekšējā dokumentu vadības sistēma.

Piemēram, vidēja izmēra ražošanas uzņēmumam ir sistēma, kur glabā iekšējos dokumentus:

Rīkojumus, līgumprojektus, komercnoslēpuma informāciju, kā arī darbinieku personu lietas. Pieņemsim, ka šis uzņēmums ir svarīgo pakalpojumu sniedzējs (t.i., attiecas likums, bet nav "kritiskā infrastruktūra").

Konfidencialitātes drošības klase: sistēmas saturs nav publisks; tur ir gan darbinieku dati (parasti personas dati), gan komercinformācija. Tie nav valsts noslēpumi, bet noteikti ierobežotas pieejamības informācija – tikai uzņēmuma iekšienē lietojama. Saskaņā ar klasifikāciju tas piešķir B konfidencialitāti.

Integritātes drošības klase: ja uzņēmuma iekšējos dokumentos tiktu veiktas izmaiņas (piemēram, līgumu teksti, rēķini), tas varētu radīt juridiskas un operacionālas problēmas, taču neapturētu uzņēmuma pamatdarbību uzreiz. Būtu jāpieliek pūles kļūdu labošanai, iespējams, rastos finansiālas vai reputācijas sekas, taču nekas neatgriezenisks. Tā kā integritātes pārkāpums būtiski neietekmē pašu pakalpojumu sniegšanu (ražošana turpinātos, tikai administrācijā haoss) un citi subjekti arī necietīs, var klasificēt C integritāti.

Pieejamības drošības klase: ja dokumentu sistēma nebūtu pieejama, piemēram, nedēļu, uzņēmums varētu turpināt ražošanu (cehs strādā, produkts top), tikai administratīvā puse bremzētos – darbinieki netiek pie saviem failiem, jāatliek atskaišu sagatavošana utt. Tas nav kritiski īstermiņā. Tātad pieejamība var būt C – drīkstētu būt garāki pārtraukumi par 1% mēnesī, īpaši ja uzņēmums apzināti plāno, piemēram, naktīs vai brīvdienās sistēmu apturēt uz uzturēšanu.

B/C/C – pamata drošība ar pastiprinātu piekļuves kontroli komercnoslēpumiem (pietiek ar pamata rezervēm un iekšēju incidentu apstrādi). Informācijas sistēmas kopējā klase ir B.

<u>Piemērs 3:</u> Iedzīvotāju reģistra valsts informācijas sistēma.

Piemēram, valsts mēroga informācijas sistēma, kurā tiek glabāti visu Latvijas iedzīvotāju personas dati.

Konfidencialitātes drošības klase: Sistēma satur konfidenciālu informāciju, ņemot vērā, ka sistēmā tiek glabāti sensitīvi personu dati (vārds, uzvārds, personas kods, dzīvesvietas adrese, pilsonība, ģimenes stāvoklis utt.). Konfidencialitātes klase būtu A, jo šādu datu noplūde var radīt personas datu aizsardzības pārkāpumus u.c.

Integritātes drošības klase: Datu precizitāte un nemainīgums ir kritiski svarīgi, jo dati tiek izmantoti citās valsts IS (piemēram, vēlēšanu sarakstos, pasu izsniegšanā). Integritātes drošības klase būtu A, jo integritātes pārkāpums var radīt virkni problēmu, ņemot vērā, ka dati sistēmā tiek ievadīti un atjaunināti pēc oficiāliem dokumentiem, piemēram, dzimšanas apliecības, tiesas nolēmuma vai laulības apliecības, kā arī izraisīt sociālās sekas (iedzīvotāji netiek iekļauti reģistros, nesaņem pakalpojumus u.c.)

Pieejamības drošības klase: Sistēmas nepieejamība radītu nopietnas sekas un iedzīvotāju reģistra IS nevarētu izsniegt personu apliecinošus dokumentus (ID kartes, pases), nevarētu reģistrēt dzīvesvietu, izmaiņas ģimenes stāvoklī (laulības, dzimšanas, miršanas). Pieejamību var ietekmēt gan pakalpojumatteices kiberuzbrukumi (DDoS), gan tehniskas problēmas. Ņemot vērā, ka tā rezultātā var rasties administratīvo procesu aizkavēšanās, pakalpojumu nepieejamība, ietekmēts arī citu iestāžu darbs, un, ņemot vērā to, ka iedzīvotāju reģistra IS pieejamo informāciju izmanto dažādas valsts iestādes, piemēram, PMLP, pašvaldības, policija utt., pieejamības drošības klase būtu A.

A/A/A – Nepieciešama stingra piekļuves kontrole, vairāku faktoru autentifikācija, regulāra drošības uzraudzība un incidentu pārvaldība ar ārēju auditu iesaisti. Jānodrošina spēja atjaunoties iepriekšējā dienā, pirms nedēļas, pirms mēneša, iepriekšējā gadā (vecāku par 365 dienām), ģeogrāfiski jāatdala rezerves resursi un jānodrošina nepārtraukta pieejamības veiktspēja.

5.2. ĀRPAKALPOJUMA UN PRIVĀTĀS INFORMĀCIJAS SISTĒMU UZSKAITE

Pārvaldnieka atbildības apjoms ir tieši saistīts ar viņam piešķirto tiesību un pilnvaru robežām, kas uzraudzības kontekstā atbilst noteikumu 54. punktam un spējai reaģēt uz incidentiem, tāpat arī vai nodrošināt ārpakalpojumu pārvaldību vai sakārtot līgumu attiecības tādā mērā, ka MK 397 prasības (atbilstoši resursa kategorijas drošības klases aizsardzības prasībām) tiek īstenotas.

Ārpakalpojumi, kuru informācijas sistēmu konfigurācija un žurnālfailu pārvaldība neatrodas subjekta tiesiskā īpašnieka vai valdītāja pārvaldībā vai kontrolē, un līdz ar to neatbilst un nespēj īstenot MK 397 54. punktā noteiktās prasības (par kiberdrošības pārvaldnieka tiesībām), nav uzskaitāmi IKT resursu un informācijas sistēmu katalogā.

Šādos gadījumos kiberdrošības politikā (t.sk. pakalpojuma vai operacionāla līmeņa līgumos) ir jānosaka organizatoriskās un administratīvās kontroles, kas nodrošina lietotāju tiesību piešķiršanas un izmantošanas uzraudzību, kā arī ārpakalpojumu un to piegāžu ķēžu drošību.

Savukārt ārpakalpojumi, kuru informācijas sistēmu konfigurācija un žurnālfailu pārvaldība atrodas subjekta tiesiskā īpašnieka vai valdītāja pārvaldībā vai kontrolē, un kas atbilst un spēj īstenot MK 397 54. punktā noteiktās prasības, ir uzskaitāmi IKT resursu un informācijas sistēmu katalogā.

<u>Piemērs 1:</u> Pašvaldības lietvedības sistēma "DokPro" (pašu pārvaldībā):

- **Īpašnieks/valdītājs:** Pašvaldības dome (īpašnieks / tiesiskais valdītājs).
- **Drošības klase (vidēja)**: B (ietekmē būtiskus procesus, satur personas datus).
- **Resursu tips**: informācijas sistēma, izvietota pašvaldības serverī.
- **Saskarnes**: integrācija ar privāto pakalpojumu e-pakalpojumu risinājumu (ārpakalpojums).
- **Pieejas tiesības:** lomas – lietvedis, vadītājs, administrators un lokāli nodrošināts MFA.
- **Rezerves kopijas**: nodrošina pašvaldības IKT nodaļa.

PIEZĪMES: Informācijas sistēma obligāti jāiekļauj katalogā, jo ir pašvaldības pārvaldībā un kontrolē, kā arī pašvaldība ir īpašnieks.

Atrodas kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā.

<u>Piemērs 2:</u> – "Horizon" (Visma SaaS ārpakalpojums):

- **Īpašnieks/valdītājs:** Visma (pašvaldībai nav īpašuma tiesības).
- **Pieejas tiesības:** Pašvaldībai ir tikai lietotāja tiesības (nespēj īstenot MK 397 54. punktā noteiktās tiesības).

PIEZĪMES: Informācijas sistēma nav jāiekļauj katalogā, jo nav pašvaldības pārvaldībā un kontrolē, kā arī pašvaldība nav īpašnieks.

Dokumentācijā (ārpakalpojumu sarakstā, piekļuves un pārvaldības procedūrā) **fiksē**:

- Kādi lietotāji/lomas tiek piešķirtas (grāmatvedis, algu speciālists, uc.).
- Kā tiek pieprasīta/atsaukta piekļuve.
- Kāds autentifikācijas veids tiek izmantots.
- Kādus drošības pasākumus (MFA, audita žurnāli, uc.) uztur pakalpojuma sniedzējs.
- Saskarnes ar citām IS (piem., adrešu dati, maksājumu saskarnes).
- Atsauce uz līgumu (SLA, piegādes ķēdes, pieejamība, incidentu ziņošana, pārvaldība, uc.).

Neatrodas kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā.

Ja autentifikācijai tiek izmantota pārvaldībā un kontrolē esoša informācijas sistēma, tad to pievieno IKT resursu un informācijas sistēmu katalogā ar aprakstu par tās funkcionalitāti.

<u>Piemērs 3:</u> – "Vienotā pašvaldību sistēma (VPS)" nozares sistēma:

- **Īpašnieks/valdītājs:** Lietojumprogrammas tiesiskais īpašnieks vai deleģēta persona.
- **Pieejas tiesības:** Pašvaldībai ir lietotāja tiesības (nespēj īstenot MK 397 54. punktā noteiktās tiesības).

Dokumentācijā (ārpakalpojumu sarakstā, piekļuves un pārvaldības procedūrā, līgumos) **fiksē**:

- Kādi lietotāji/lomas tiek piešķirtas (grāmatvedis, algu speciālists).
- Kā tiek pieprasīta/atsaukta piekļuve.
- Kāds autentifikācijas veids tiek izmantots.
- Kādus drošības pasākumus (MFA, audita žurnāli, uc.) nodrošina pakalpojuma sniedzējs.
- Saskarnes ar citām IS (piem., adrešu dati, maksājumu saskarnes, uc.).
- Atsauce uz līgumu (SLA, piegādes ķēdes, pieejamība, incidentu ziņošana, pārvaldība, uc.).

Neatrodas kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā.

Ja autentifikācijai tiek izmantota pārvaldībā un kontrolē esoša informācijas sistēma, tad to pievieno IKT resursu un informācijas sistēmu katalogā ar aprakstu par tās funkcionalitāti.

Piemērs 4: – Kiberdrošības riskam pakļauta pašvaldības tīkla infrastruktūra.

Piemēram: Tīkla ierīce, kas nodrošina datu plūsmu vadību starp dažādiem loģiskajiem vai fiziskajiem tīkla segmentiem, ugunsmūris, u.c.

- **Resursu tips**: Tehniskais resurss.
- **Īpašnieks:** Pašvaldības dome (īpašnieks / tiesiskais valdītājs).
- **Drošības klase:** saskaņā ar augstākās drošības klases informācijas sistēmu.
- **Pieejas tiesības:** administratoru saraksts, piekļuves procedūra.

Atrodas kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā.

6. BUJ

1. **Saskaņā ar Ministru kabineta noteikumu Nr. 397 34. pantu: "Kritiskās infrastruktūras kopumā iekļautu informācijas sistēmu uzskata par A drošības 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 drošības klases informācijas sistēmas.
   Vai šādā gadījumā ir nepieciešams aizpildīt 5. pielikumu, kas paredzēts drošības klases izvērtēšanai?

   Atbilde: Vēršam uzmanību uz MK 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 noteikumu 5. pielikumā ietverto metodiku. Ņemot vērā norādīto subjektam nepieciešams noteikt 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, un saskaņā ar MK 397 35. punktā noteikto, nosūtīt tās saskaņošanai SAB.

2. **Kritiskās infrastruktūras 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 drošības klases iekārtām?**

Atbilde: Skaidrojam, ka Ministru kabineta 2021. gada 6. jūlija noteikumi Nr. 508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība" (turpmāk - MK noteikumi Nr. 508) 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. 508 ietvertā kritiskās infrastruktūras klasifikācija izriet no Nacionālās drošības likuma $22.^2$ panta otrajā daļā ietvertās klasifikācijas. Skaidrojam, ka, piemēram, gadījumā, ja MK noteikumu Nr. 508 izpratnē tiek piešķirta B kategorijas kritiskās infrastruktūras statuss, tas nenozīmē, ka visām sistēmām MK 397 izpratnē arī tiks piešķirta B drošības klase.

3. **Kritiskās infrastruktūras 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?**

Atbilde: Ja 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 saskaņā ar MK 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 drošības klases par A drošības klasi.

4. **Gadījumā, ja mēs kā iestāde esam noteikti par kritisku infrastruktūru (B kategorijas), tajā esošās informācijas sistēmas, saskaņā ar Ministru kabineta noteikumu Nr. 397 34. pantu, automātiski jāuzskata par A drošības klases sistēmām?**

Atbilde: Ministru kabineta 2021. gada 6. jūlija noteikumi Nr. 508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība" (turpmāk – MK noteikumi Nr. 508) 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. 508 ietvertā kritiskās infrastruktūras klasifikācija izriet no Nacionālās drošības likuma 22.2. panta otrajā daļā ietvertās klasifikācijas. Skaidrojam, ka, piemēram, gadījumā, ja MK noteikumu Nr. 508 izpratnē tiek piešķirta B kategorijas kritiskās infrastruktūras statuss, tas nenozīmē, ka visām sistēmām MK 397 izpratnē arī tiks piešķirta B drošības klase.

5. **Es pareizi saprotu, ka tehniskajiem resursiem nav jānosaka konfidencialitātes, integritātes un pieejamības drošības klase (A, B vai C) atbilstoši MK 397 noteikumu 5. pielikumā ietvertajai metodikai?**

Atbilde: Jā, tehniskajiem resursiem (piemēram, tīkla ierīcēm) nav jāpiešķir A/B/C drošības klase saskaņā ar MK 397 32. punktu, jo klasifikācija attiecas tikai uz informācijas sistēmām un informācijas resursu kategorijām. Tomēr tehniskie resursi manto klasi no tās informācijas sistēmas piederības. Piemēram, tehniskais resurss “Cisco router” pieder pie B drošības klases informācijas sistēmas un ir klasificējams kā B drošības klases tehniskais resurss un uz to attiecas, piemēram, B drošības klases ārpakalpojuma prasības.

6. **Konfidencialitātes, integritātes un pieejamības drošības klasi nosaka katram informācijas resursam / informācijas resursu kategorijai un katrai informācijas sistēmai?**

Atbilde: Pēc MK 397 32. punkta nosacījumiem konfidencialitātes, integritātes un pieejamības klase tiek noteikta katrai informācijas sistēmai un katrai informācijas resursu kategorijai tās sastāvā. Tas nozīmē, ka katrai informācijas sistēmai un katrai kategorijai (piem., personu datu apstrādes serveris, "ierobežota pieejamība" informācija utt.) ir jānosaka atbilstošā A/B/C klase.

7. **Lūdzam paskaidrot noteikumu 32. punktā minēto jēdzienu "informācijas resursu kategorija".**

Atbilde: Tās var būt, piemēram, publiski pieejami dati, personas dati, komerciālas slepenas ziņas, "Ierobežotas pieejamības" informācija utt. MK 397 32. punkts paredz katrai sistēmai un katrai tās apstrādāto informācijas resursu kategorijai piešķirt drošības klasi. Resursu kategoriju piemēri nav tieši definēti MK 397, taču tās saprot kā informācijas veidus vai grupa ar līdzīgu aizsardzības līmeni.

8. **Informācijas sistēmai konfidencialitātes, integritātes un pieejamības drošības klasi nosaka, pamatojoties uz to, kāda (augstākā) klase ir piešķirta šajā sistēmā dzīvojošiem informācijas resursiem? Vai var būt izņēmumi?**

Atbilde: Saskaņā ar MK 397 33. punktu informācijas sistēmas kopējā A/B/C klase tiek noteikta pēc augstākā tās apstrādāto resursu drošības klases (augstākais riska līmeņa kritērijs). Tātad ja kādam informācijas resursam sistēmā klasifikācijā piešķirta A konfidencialitātes (vai integritātes vai pieejamības) klase, visa sistēma ir A klase. Izņēmumu 34. punkts paredz tikai kritiskās infrastruktūras sistēmām (automātiski A klase), citādi sistēmas klase vienmēr balstās uz augstāko resursa klasi.

9. **Veicot IS klasifikāciju identificējam, ka ir arī IS, kuru vērtējums pēc konfidencialitātes, integritātes, pieejamības būtu pat zemāks kā C drošības klases gadījumā un kuras neiespaido organizāciju kā mobilo sakaru pakalpojuma sniedzēja sniegto pakalpojumu (sakarus, SMS, pārraidītos datus). Izrietoši no tā organizācijas juristi un IT departamenta vadība uzskata, ka šādas sistēmas ir ārpus klasifikācijas tvēruma un nav iekļaujamas IS katalogā.**

Atbilde: MK 397 30. punkts prasa uzskaitīt un klasificēt visas IKT resursus un informācijas sistēmas, kas pakļautas kiberriskiem. Nav paredzēts izņēmums sistēmām ar "mazāku par C" vērtējumu. Ja kāda sistēma atrodas pakļauta kiberriskam, tai jāpiešķir klase saskaņā ar 32. un 33. punktu metodiku. Tātad arī organizācijā minētās sistēmas jāiekļauj katalogā un jāklasificē (ja nepieciešams, piešķirot zemāko C klasi).

10. **Vai IS var netikt piešķirta drošības klase (A, B vai C), ja tā neatbilst nevienai no konfidencialitātes, integritātes, pieejamības klasēm? Vai IS, kuras neatbilst nevienai no konfidencialitātes, integritātes, pieejamības klasēm, var neiekļaut IS katalogā?**

Atbilde: MK 397 32. punkts prasa klasificēt katru kiberriskam pakļauto informācijas sistēmu (un resursu kategoriju). Ja kāda sistēma nav nevienas drošības klases kritēriju piemērota, MK 397 neparedz īpašu "nedefinēto" statusu vai izslēgšanu no kataloga. Tādejādi visām sistēmām tomēr tiek piešķirta vismaz C klase (pamata), un tās jāiekļauj IS katalogā.

11. **Vai rezerves kopijas (69.2., 69.3. punktā minētās) būtu uzskatāmas par informācijas resursu vai tehnisko resursu MK 397 noteikumu izpratnē?**

Atbilde: MK 397 69. punkts skaidro rezerves kopiju prasības, tajā 69.2. punktā piemin rezerves kopijas atvērtā koda bibliotēku pirmkoda (t.i. informācijas sistēmas programmatūras) versijām, bet 69.3. punktā – tehnisko resursu konfigurācijas kopijas. Tāpēc 69.2. attiecināms uz informācijas resursiem (sistēmas kods), savukārt 69.3. attiecināms uz tehniskajiem resursiem (sistēmas darbību nodrošinošo tehnikas uzstādījumi).

12. **Par kritiskās infrastruktūras IS drošības klases iedalījumu, ja KI īpašnieks ir klasificēts kā B drošības klases kritiskā infrastruktūra, vai visas attiecīgās KI informācijas sistēmas automātiski tiek uzskatītas par A drošības klases sistēmām atbilstoši MK 397 prasībām?**

Atbilde: MK 397 34. punkts paredz A klasi tikai IKT kritiskās infrastruktūras kopumā iekļautām sistēmām. Tas neparedz automātiski klasificēt kā A drošības klases visas iestādes sistēmas. Ja kritiskā infrastruktūra kā tāda ir B kategorijas, tas pats princips – tikai sistēmas, kas kvalificētas kā kritiskās infrastruktūras daļa, tiek definētas kā A drošības klases, ja vien SAB nav saskaņojis savādāk, bet pārējās parastajā kārtībā saskaņā ar 32.–33. punktu.

13. **Vai pareizi saprotu, ka tad, ja subjekts ir kritiskā infrastruktūra, bet ne IKT kritiskā infrastruktūra, tad tajā gadījumā visas subjekta valdījumā un īpašumā esošas IS ir A klases IS? Vai arī tikai tās IS, kas ir iekļautas kritiskās infrastruktūras kopumā, tādā gadījumā, kā var izdalīt, kuras sistēmas ir iekļautas kopumā?**

Atbilde: Ja subjekts ir klasificēts kā kritiskā infrastruktūra bet ne IKT kritiskā infrastruktūra, tas pats princips – A drošības klases statuss automātiski pienākas tikai kritiskajai infrastruktūrai iekļautajām IS, ja vien SAB nav saskaņojis savādāk. Tātad netiek automātiski padarītas par A drošības klases vismazākās sistēmas – jāvērtē, kuras sistēmas nodrošina kritiskos pakalpojumus un tiek definētas kā kritiskās infrastruktūras IS. IKT kritiskajā infrastruktūrā drošības klases saskaņo ar SAB.

14. **Vēlētos precizēt, vai grāmatvedības (ERP) sistēma svarīgajiem pakalpojumu sniedzējiem ir A vai B drošības klases drošības klase un vai ir pieejami skaidri nosacījumi, uz kuriem var nošķirt, kura klase būtu jāpiemēro?**

Atbilde: ERP sistēmas klasei nav iepriekš noteikta algoritma. Tā jāklasificē kā jebkura sistēma pēc MK 397 33. punkta kritērijiem. Ja ERP satur "Ierobežotu pieejamību" vai daudz personu sensitīvus datus, tai var būt A klase. Ja tajā apstrādāti, piemēram, personas dati bez papildu augsta līmeņa riskiem, iespējams B klase. Informācijas sistēmas drošības klase seko MK 397 klasifikācijai – A, B vai C sistēmas klasifikācija seko atkarībā no tās augstākā riska līmeņa piešķirtā A/B/C kritērija.

15. MK 397 35. punktā noteikts: "Ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar Satversmes aizsardzības biroju". **Lūgums skaidrot - Vai klasifikācija veicama subjekta īpašumā un valdījumā esošajām visām IS vai tikai tām IS, kas ietilpst subjekta kritiskajā infrastruktūrā un tiek izmantotas kritisko pakalpojumu nodrošināšanai?**

Atbilde: Ar Satversmes aizsardzības biroju visas drošības klases jāsaskaņo tikai tad, ja visa subjekta IKT infrastruktūra faktiski ir kritiskās infrastruktūras kopumā iekļauta (t.i., piemēro 35. punkta nosacījumu). Tas nozīmē, ka šajā gadījumā visas subjekta IS pakļaujas kritiskās infrastruktūras režīmam. Ja kritiskajā infrastruktūrā iekļautas tikai dažas IS, par kurām noteikta A klase, tad pārējo riskam pakļauto informācijas sistēmu un resursu drošības klases saskaņojums ar SAB nav nepieciešams.

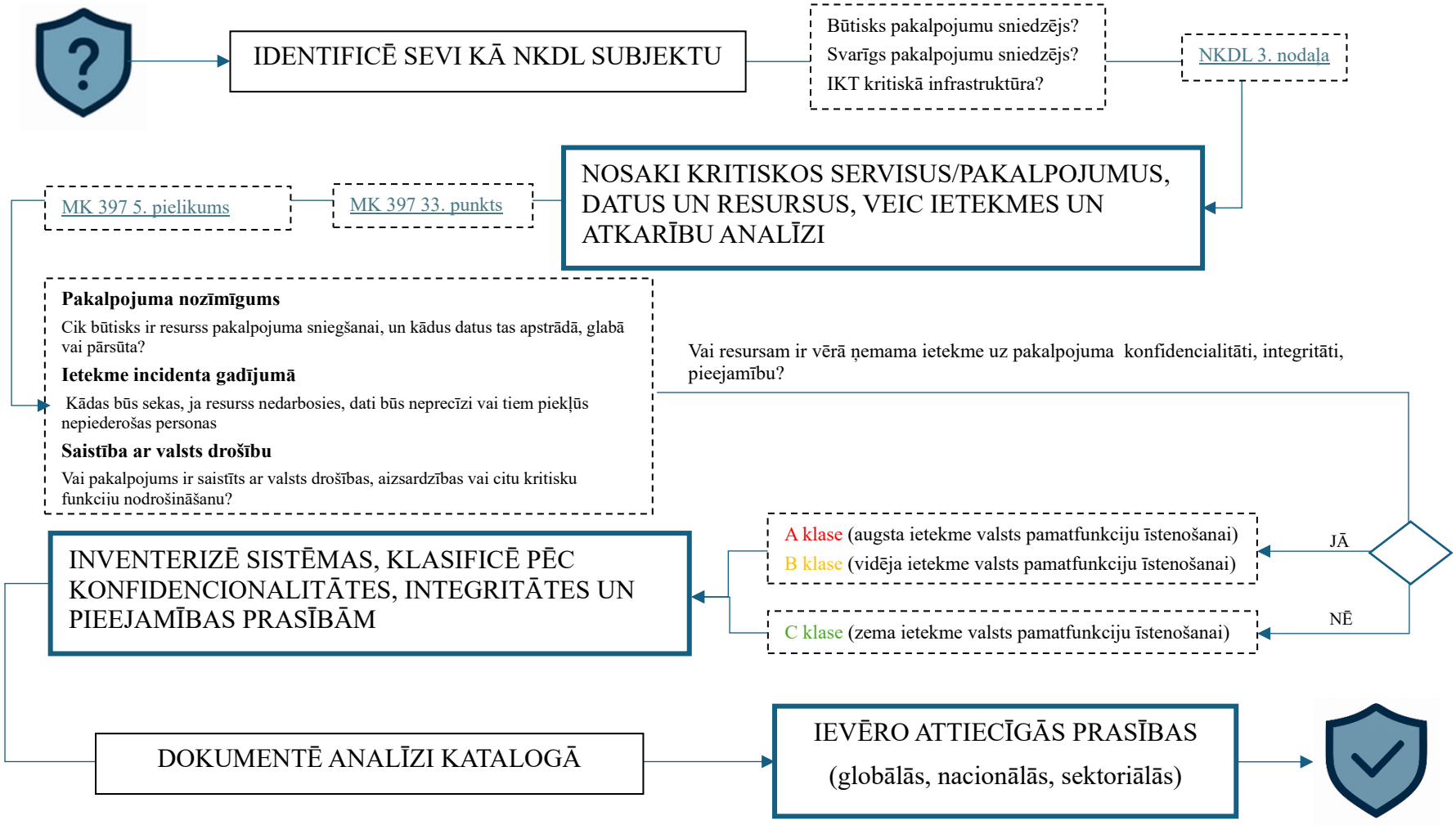
16. Vai nosakot sistēmas klasi ir jāuzskata, ka starp pazīmēm ir loģiskais "un" vai "vai"? T.i., lai noteiktu, piemēram, A drošības klases konfidencialitāti ir jāizpildās visām trīs pazīmēm, kas minētas 5. pielikumā, vai pietiek ar vienu no šīm pazīmēm?

Atbilde: Saskaņā ar 5. pielikumu katrai drošības klasei ir uzskaitītas vairākas neatkarīgas pazīmes. Lai informācijas sistēma būtu piemērota A drošības klases konfidencialitātei, viena no A drošības klases pazīmēm pietiek. Piemēram, ja sistēmas dati satur vismaz 1 000 000 personas datu, tā jau atbilst A drošības klases konfidencialitātes kritērijiem. Nav vajadzīgs, lai vienlaikus tiktu izpildītas visas tabulā uzskaitītās pazīmes. Šīs pazīmes darbojas kā "vai" nosacījumi. 5. pielikuma tabulā redzams, ka A/B/C klasi piešķir, ja atbilst vismaz vienai no attiecīgajā klasē minētajām pazīmēm (kritērijiem) un klasificē pēc augstākās riska līmeņa dimensijas.

7. IETEIKUMI

7.1. Darbību plāns subjektiem

1. Inventarizēt resursus un sistēmas, balsoties uz nozīmīgiem kiberdrošības riskam pakļautiem procesiem, pakalpojumiem, kiberrisku analīzi un drošības klasēm.
2. Piešķirt drošības klases atbilstoši metodikai un pamatot, dokumentējot to tabulā (IKT resursu un informācijas sistēmu katalogs).
3. Modelēt kritisko pakalpojumu un ar tiem saistīto informācijas glabāšanas, apstrādes un pārsūtīšanas sistēmu arhitektūru, lai identificētu potenciālos apdraudējuma laukumus, ievainojamības un ar tiem saistītos riskus.
4. Saskaņot un koordinēt kontroles ar klasēm (MFA, žurnālfaili, rezerves, piegāžu ķēžu pārvaldība, ārpakalpojumi utt.).
5. Sekot ENISA norādēm un nozares regulatoru prasībām.
6. Pārskatīt dokumentāciju un kiberrisku pārvaldības, un nepārtrauktības plānus vismaz reizi gadā vai būtisku izmaiņu gadījumā.
7. Sekot līdzi aktualitātēm vietnēs *cyber.gov.lv* un *cert.lv*, lai savlaicīgi saņemtu informāciju par jaunākajām norādēm un drošības ieteikumiem.



Identifikācija (aktīvi/pakalpojumi)→ **ietekme/atkarības → klasifikācija → prasības/kontroles → dokumentēšana → pārskatīšana**