KIBERDROŠĪBAS TIESISKIE ASPEKTI LATVIJAS TIESĪBU REGULĒJUMĀ

Foto no personīgā arhīva

Mg. iur. **Paula Kellija**
ZAB "Ellex Kļaviņš" juriste

IEVADS

Digitalizācija rada jaunas iespējas un atvieglo uzņēmumu un iestāžu iekšējo procesu pārvaldību, to efektivizējot, tomēr vienlaikus tā rada arī jaunus izaicinājumus, tostarp noturību pret kiberuzbrukumiem. Saskaņā ar Eiropadomes datiem 2020. gadā kibernoziedzības radītās globālās ekonomiskās izmaksas sasniedza divkāršu apmēru salīdzinājumā ar 2015. gadu.[1]

Reaģējot uz kiberdraudu pieaugumu mūsdienu digitālajā vidē un konstatētajiem trūkumiem esošajā kiberdrošības regulējumā, Eiropas Savienībā (turpmāk – ES) 2023. gada 16. janvārī stājās spēkā Direktīva (ES) 2022/2555[2] (turpmāk – NIS2 direktīva). Tās mērķis ir ieviest stingrākas un vienotas drošības prasības kiberdrošības jomā visā ES. NIS2 direktīva aizstāj iepriekšējo NIS direktīvu – Direktīvu (ES) 2016/1148,[3] kuras izstrāde sākotnēji bija liels solis kiberdrošības noturības veicināšanā Eiropas līmenī.

Lai transponētu NIS2 direktīvu nacionālajos tiesību aktos, 2024. gada 1. septembrī Latvijā stājās spēkā Nacionālais kiberdrošības likums[4] (turpmāk – Kiberdrošības likums), bet 2025. gada 2. jūlijā stājās spēkā Ministru kabineta noteikumi Nr. 397 "Minimālās kiberdrošības prasības"[5] (turpmāk – Minimālās kiberdrošības prasības), nosakot konkrētas tehniskās un organizatoriskās prasības, kuras ir jāievēro Kiberdrošības likuma subjektiem. Jaunais regulējums būtiski maina līdzšinējo tiesisko regulējumu Latvijā kiberdrošības jomā. Tas ir nopietns solis pretim noturīgākai digitālajai videi pret kiberdraudiem un kiberuzbrukumiem, kas ir jo īpaši būtiski ģeopolitisko notikumu kontekstā. Šajā rakstā aplūkotas autores ieskatā galvenās jaunās regulējuma tvēruma nianses un prasības, kas noteiktas Kiberdrošības likumā un Minimālajās kiberdrošības prasībās.

1 Eiropadome un Eiropas Savienības Padome. Kiberdraudi Eiropas Savienībā: fakti un skaitļi. Pieejams: *https://www.consilium.europa.eu/en/policies/top-cyber-threats/*

2 Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā. OV L 333, 27.12.2022.

3 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. OV L 194, 19.07.2024.

4 Nacionālais kiberdrošības likums. Latvijas Vēstnesis, 04.07.2024, Nr. 128A.

5 Ministru kabineta 2025. gada 25. jūnija noteikumi Nr. 397 "Minimālās kiberdrošības prasības". Latvijas Vēstnesis, 01.07.2025., Nr.123.

1. NACIONĀLĀ KIBERDROŠĪBAS LIKUMA SUBJEKTI

Stājoties spēkā NIS2 direktīvai, paplašināts arī nozaru loks, uz kurām attiecas kiberdrošības regulējuma prasības. Tagad kiberdrošības regulējums aptver arī tādas jomas kā atkritumu apsaimniekošana, pārtikas ražošana un izplatīšana, pasta un kurjerpasta pakalpojumi, ražošana sabiedrībai nozīmīgās nozarēs (piemēram, zāļu un medicīnisko ierīču ražošana), kā arī informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) pārvaldības un kiberdrošības pakalpojumi. Jānorāda, ka visas nozares, uz kurām attiecas NIS2 direktīva, ir uzskaitītas tās pirmajā un otrajā pielikumā.

Kiberdrošības likums šīs nozares klasificē trīs grupās: būtisko pakalpojumu sniedzēji, svarīgo pakalpojumu sniedzēji un IKT kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji.

Saskaņā ar Kiberdrošības likuma 20. pantu par būtisko pakalpojumu sniedzējiem ir uzskatāmi, piemēram, elektronisko sakaru komersanti, kvalificētu uzticamības pakalpojumu sniedzēji, sabiedriskie elektroniskie plašsaziņas līdzekļi, kredītiestādes, ārstniecības iestādes un lieli saimnieciskās darbības veicēji, kuri ir, piemēram, energoapgādes vai naftas komersanti.

Potenciālā subjekta izvērtēšanas procesā komersanta statuss kā vidējam vai lielam saimnieciskās darbības veicējam tiek noteikts, pamatojoties uz Kiberdrošības likuma 20. panta astotajā punktā noteiktajiem kritērijiem. Minētais regulējums atspoguļo NIS2 direktīvas 3. panta 1. punkta a) apakšpunktu, saskaņā ar kuru par būtisko pakalpojumu sniedzējiem uzskatāmi Direktīvas I pielikumā minētie pakalpojumu sniedzēji, kas pārsniedz vidēja uzņēmuma maksimālo lielumu, kā tas noteikts Eiropas Komisijas 2003. gada 6. maija ieteikumā 2003/361/EK[6] (turpmāk – Ieteikums). Saskaņā ar Ieteikuma pielikuma 2. panta 1. punktu par lieliem uzņēmumiem uzskatāmi uzņēmumi, kuros: 1) ir vairāk nekā 250 darbinieku; 2) gada apgrozījums pārsniedz 50 miljonus eiro vai 3) gada bilances kopsumma pārsniedz 43 miljonus eiro. Attiecīgi šādi uzņēmumi Latvijas tiesiskajā regulējumā tiek kvalificēti kā būtisko pakalpojumu sniedzēji, ja tie darbojas Kiberdrošības likuma 20. panta astotajā daļā minētajās nozarēs. Lai gan Ieteikumā vidēja uzņēmuma definīcija nav izteikta tieši, to interpretējot, par vidēju uzņēmumu uzskatāms uzņēmums, kurā: 1) ir mazāk nekā 250 darbinieku, 2) gada apgrozījums vai bilances kopsumma nepārsniedz 50 miljonus eiro, 3) bet pārsniedz mazā uzņēmuma robežas (10 miljonus eiro). Šī pieeja nacionālajā regulējumā ir nostiprināta Kiberdrošības likuma 1. panta 25. punktā, kas nosaka, ka par vidēju saimnieciskās darbības veicēju uzskatāms komersants, kurš nodarbina līdz 249 darbiniekiem un kura gada apgrozījums ir no 10 līdz 50 miljoniem eiro vai gada bilances kopsumma ir no 10 līdz 43 miljoniem eiro.

> NEPIETIEKAMA KIBERDROŠĪBAS RISKU PĀRVALDĪBA VAR RADĪT IEVĒROJAMUS FINANSIĀLUS ZAUDĒJUMUS, JURIDISKAS SEKAS, TOSTARP STRĪDUS PAR PERSONAS DATU AIZSARDZĪBAS PĀRKĀPUMIEM VAI DROŠĪBAS PRASĪBU NEIEVĒROŠANU, KĀ ARĪ NOZĪMĪGU REPUTĀCIJAS RISKU UZŅĒMUMAM.

Papildus ir jāpiemin, ka par būtisko pakalpojumu sniedzējiem ir uzskatāmas arī atvasinātas publiskas personas, tiešās pārvaldes iestādes un citas valsts institūcijas, kā arī privāto tiesību juridiskās personas, kas pilda valsts pārvaldes deleģētu uzdevumu, izņemot valsts drošības iestādes un pastarpinātās pārvaldes iestādes, kuras sniedz pakalpojumus vai darbojas privāto tiesību jomā kādā no Kiberdrošības likuma 20. panta astotajā daļā minētajām jomām.

Atbilstoši Kiberdrošības likuma 21. pantam par svarīgo pakalpojumu sniedzējiem uzskatā-

6 Eiropas Komisijas 2003. gada 6. maija ieteikums par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju 2003/361/EK. OV L 124, 20.05.2003.

mi tie komersanti, kuri atbilst vidēja lieluma saimnieciskās darbības veicēja kritērijiem un veic komercdarbību kādā no Kiberdrošības likuma 20. panta astotajā daļā minētajām nozarēm. Par svarīgo pakalpojumu sniedzējiem ir uzskatāmi arī tādi komersanti, kuri ir vidēji vai lieli un kuri ir pasta komersanti, atkritumu apsaimniekotāji, datoru, elektronisko iekārtu ražotāji, tiešsaistes tirdzniecības vietas pakalpojumu sniedzēji un citi komersanti, kas ir norādīti šajā otrajā daļā. Kā arī svarīgo pakalpojumu sniedzēji ir pastarpinātās pārvaldes iestādes, kuras sniedz pakalpojumus vai darbojas privāto tiesību jomā vismaz vienā no Kiberdrošības likuma 21. panta pirmās daļas 2. punktā minētajām jomām.

Par IKT kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem uzskatāmas personas, kuru IKT sistēmas ir iekļautas Ministru kabineta apstiprinātajā kritiskās infrastruktūras kopumā un kurām pieder vai kuras pārvalda valsts nozīmes tehnoloģiju un sistēmu elementus, piemēram, datu centrus, interneta pamattīklus, mobilo un fiksēto sakaru tīklus, kā arī digitālās identifikācijas risinājumus. Uz šīm personām attiecināmas Ministru kabineta noteiktās IKT kritiskās infrastruktūras drošības prasības, kas nedrīkst būt zemākas par šajā likumā noteiktajām prasībām būtisko pakalpojumu sniedzējiem.

Par IKT infrastruktūras objektiem tiek atzīti tādi tehnoloģiskie resursi un sistēmas, kas nodrošina būtisku valsts un sabiedrības funkciju nepārtrauktu darbību un kuru bojājumi, darbības traucējumi vai iznīcināšana varētu radīt nozīmīgu kaitējumu valsts vai sabiedrības interesēm.

Jaunā regulējuma prasības neattiecas uz elektronisko sakaru tīklos pārraidīto informācijas saturu, tostarp informācijas sabiedrības pakalpojumu un audiovizuālo saturu, izņemot gadījumus, kad šis saturs tiek izmantots kā kiberincidenta sastāvdaļa. Tāpat regulējums neattiecas uz būtisko vai svarīgo pakalpojumu sniedzējiem, kuri vienlaikus atbilst visiem šādiem nosacījumiem: (i) pakalpojumu sniedzējs ir reģistrēts kādā Eiropas Savienības dalībvalstī, un tā galvenā reģistrācijas vieta nav Latvija; (ii) Latvijā tas sniedz tikai tos pakalpojumus, kas ir konkrēti minēti Kiberdrošības likuma 20. panta 1. un 2. punktā, 8. punkta "s–v" apakšpunktā, kā arī 21. panta attiecīgajos apakšpunktā; (iii) tas Latvijā nesniedz citus būtiskos vai svarīgos pakalpojumus; un (iv) tas nav IKT tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

Ikvienam uzņēmumam būtu jāizvērtē sava atbilstība kādam no Kiberdrošības likumā noteiktajiem subjektu veidiem. Konstatējot atbilstību, uzņēmumam ir nekavējoties pienākums reģistrēties Nacionālajā kiberdrošības centrā (turpmāk – NKDC), aizpildot elektroniski parakstītu statusa paziņojuma veidlapu, kas ir atrodama Minimālo kiberdrošības prasību 1. pielikumā. Atbilstoši savai kompetencei NKDC var arī paši veikt publiskajos reģistros pieejamās informācijas pirmšķietamu izvērtējumu un izsūtīt subjektam aicinājumu izvērtēt savu statusa atbilstību.

2. GALVENĀS PRASĪBAS SUBJEKTIEM KIBERDROŠĪBAS JOMĀ

Ar jaunā regulējuma spēkā stāšanos kiberdrošības jomā subjektiem ir ieviestas vairākas prasības, atbilstoši kurām subjektiem ir jānodrošina sava iekšējā dokumentācija, savu tīklu un informācijas sistēmu atbilstība.

Kiberdrošības likums nosaka vispārīgos pienākumus kiberdrošības jomā, piemēram, pienākumu iecelt kiberdrošības pārvaldnieku. Savukārt Minimālās kiberdrošības prasības detalizē tehniskos un organizatoriskos pasākumus, kā šie jaunie pienākumi kiberdrošības jomā ir praktiski īstenojami, piemēram, kādiem juridiskajiem kritērijiem ir jāatbilst kiberdrošības pārvaldniekam.

Visas jaunā regulējuma prasības uzskaitīt nebūtu iespējams, tādēļ turpmāk tiks apkūkotas tikai autores ieskatā galvenās. Papildus tam ir jāuzsver, ka saskaņā ar Kiberdrošības likumu visiem likuma subjektiem līdz 2025. gada 1. aprīlim bija jāpaziņo par savu atbilstību Kiberdrošības likuma prasībām un līdz 2025. gada 1. oktobrim bija jānozīmē kiberdrošības pārvaldnieks uzņēmumā, kā arī jāsniedz pirmais pašvērtējuma ziņojums, kurā subjekts detalizēti uzskaitītu visas līdz šim ieviestās prasības atbilstoši jaunajam regulējumam.

2.1. Kiberdrošības pārvaldnieks

Viena no būtiskajām prasībām, kas izriet no Kiberdrošības likuma, ir subjekta vadītāja pienākums noteikt atbildīgo fizisko personu – kiberdrošības pārvaldnieku, kas īsteno un pārrauga kiberdrošības pasākumu īstenošanu attiecīgajā subjektā. Tā galvenie pienākumi ir plānot un vadīt uzņēmuma vai iestādes IKT drošības pasākumus, reizi gadā pārbaudīt IKT drošību un nodrošināt, ka konstatētie trūkumi tiek novērsti, periodiski piedalīties kiberdrošības apmācībās un organizēt darbinieku instruktāžu par aktuālajiem kiberriskiem un kiberdrošību. Jo īpaši šādas instruktāžas ir jāorganizē pēc notikuša kiberincidenta.

> LATVIJĀ NACIONĀLAIS KIBERDROŠĪBAS CENTRS IR NOTEIKTS PAR VIENOTO KONTAKTPUNKTU UN KOMPETENTO IESTĀDI KIBERDROŠĪBAS JOMĀ, KĀ ARĪ TAS UZRAUGA KIBERDROŠĪBAS PRASĪBU IZPILDI BŪTISKO UN SVARĪGO PAKALPOJUMU SNIEDZĒJU UZŅĒMUMOS UN IESTĀDĒS.

Kritēriji, kuriem kiberdrošības pārvaldniekam jāatbilst atkarībā no konkrētā kiberdrošības subjekta veida, ir noteikti Minimālajās kiberdrošības prasībās. Par kiberdrošības pārvaldnieku var iecelt personu, kas atbilst noteiktajiem kritērijiem. Būtisko un svarīgo pakalpojumu sniedzēju gadījumā kiberdrošības pārvaldnieks var būt jebkuras Eiropas Savienības vai NATO dalībvalsts pilsonis, kuram ir vismaz izglītība informācijas tehnoloģiju jomā vai atbilstoša profesionālā pieredze, ko apliecina praktiskā darba pieredze vai starptautiski atzīts sertifikāts.

Jāatzīmē, ka kiberdrošības pārvaldniekam IKT kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju struktūrās ir noteiktas ievērojami stingrākas prasības. Ņemot vērā šā pārvaldnieka lomu un potenciālo ietekmi uz valstij un sabiedrībai būtisku pamatfunkciju nodrošināšanu un svarīgu pakalpojumu nepārtrauktu saņemšanu, subjektam ir pienākums nodrošināt, ka attiecīgā persona ir kompetenta, ar atbilstošu profesionālo kvalifikāciju un pieredzi, kā arī uzticama, proti, spējīga un motivēta rīkoties Latvijas valsts un sabiedrības interesēs.[7]

Par kiberdrošības pārvaldnieka nozīmēšanu subjektam ne vēlāk kā piecu darba dienu laikā ir jāpaziņo kompetentajai iestādei kiberdrošības prasību ievērošanas uzraudzībā – NKDC. IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam kandidāts iepriekš ir obligāti jāsaskaņo ar Satversmes aizsardzības biroju (turpmāk – SAB), un tikai pēc SAB piekrišanas konkrēto personu var apstiprināt darbam.

2.2. Kiberincidentu ziņošanas pienākums

Atbilstoši Kiberdrošības likuma prasībām subjektiem ir pienākums ziņot par konstatētajiem kiberincidentiem. Tas ir būtisks pienākums, jo ļauj kompetentajām iestādēm savlaicīgi identificēt apdraudējumus, to izplatību un izmantotās metodes, kā arī tas palīdz novērst līdzīgus vai tādus pašus incidentus citos subjektos. Saskaņā ar kompetentās kiberincidentu novēršanas institūcijas – Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienības CERT.LV (turpmāk – CERT.LV) – datiem, 2025. gada trešajā ceturksnī Latvijas kibertelpā no 1. jūlija līdz 30. septembrim tika reģistrēti 671 kiberincidenti. Tas ir par 5 % mazāk nekā 2025. gada otrajā ceturksnī, bet par 2 % vairāk nekā 2024. gada trešajā ceturksnī, un kopumā vērojama augšupejoša tendence.[8]

Par kiberincidentu ir uzskatāms tāds notikums, kas apdraud uzņēmuma vai iestādes apstrādātus datus vai pakalpojuma pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas. Konstatējot kiberincidentu savā tīklā, subjek-

7 Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" anotācija. Latvijas Vēstnesis, 01.07.2025., Nr. 123.

8 CERT.LV. Situācija Latvijas kibertelpā. Periods: 01.07.2025.–30.09.2025. Pieejams: *https://cert.lv/uploads/parskati/CERT_LV_parsk_C3_2025.pdf*

tam ciešā sadarbībā ar nozīmēto kiberdrošības pārvaldnieku ir jāveic visas kiberincidenta novēršanai nepieciešamās darbības un atkarībā no kiberincidenta veida jāinformē CERT.LV. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs informē arī SAB.

Atkarībā no tā, vai kiberincidents ir uzskatāms par nozīmīgu vai nenozīmīgu, iedalās tā ziņošanas prasības. Par nozīmīgu kiberincidentu atbilstoši Minimālajām kiberdrošības prasībām uzskata tādu incidentu, kas atbilst būtiska kiberincidenta definīcijai Regulas 2024/2690 3. panta 1. punkta izpratnē vai vienai no Minimālo kiberdrošības prasību 118.2. apakšpunktā minētajām pazīmēm, piemēram, kiberincidents apdraud sabiedrības drošību.

Nozīmīga kiberincidenta gadījumā subjektam 24 stundu laikā no konstatēšanas brīža CERT.LV jāiesniedz aizpildīta agrīnā brīdinājuma veidlapa, savukārt 72 stundu laikā jāiesniedz sākotnējais ziņojums, kurā sniegts iespējamo kiberincidenta cēloņu apraksts un tā ietekmes novērtējums. Savukārt, ja sešu mēnešu laikā incidentu nav izdevies novērst, subjektam jāiesniedz progresa ziņojums. Visbeidzot, sekmīga kiberincidenta atrisināšanas gadījumā sagaidāms, ka sešu mēnešu laikā kopš sākotnējā ziņojuma iesniegšanas subjektam kompetentajai institūcijai ir jāsniedz arī galaziņojums.

Kiberincidenta, kurš nav uzskatāms par nozīmīgu, gadījumā subjektam tāpat ir jāziņo par to kompetentajai institūcijai, sniedzot tādu informāciju kā notikuma apraksts, skarto iekārtu uzturētie servisi un citu informāciju, kas var palīdzēt incidenta atrisināšanā. Jebkurā gadījumā subjektam, konstatējot kiberincidentu, vispirms ir jānovērtē tā nozīmīgums.

Ja kiberincidenta rezultātā notikusi personas datu noplūde, subjektam papildus iestājas pienākums par to paziņot Datu valsts inspekcijai, kā arī bez nepamatotas kavēšanās informēt personas, kuru personas dati ir skarti. Vienlaikus subjektam ir jāveic visi nepieciešamie pasākumi, lai novērstu vai mazinātu turpmāku datu subjektu tiesību aizskārumu. Ņemot vērā, ka kiberincidentu sekas var skart ne tikai subjekta mantiskās intereses, bet arī personu pamattiesības un sabiedrības uzticību, ir īpaši būtiski, lai subjekti savlaicīgi nodrošinātu savu informācijas sistēmu noturību un ieviestu skaidras iekšējās procedūras rīcībai kiberincidentu gadījumā.

2.3. Kiberdrošības pārvaldības dokumentācija

Atbilstoši Minimālajām kiberdrošības prasībām subjektiem ir jāizstrādā un periodiski jāpārskata kiberdrošības pārvaldības dokumentācija, kuru veido šādi dokumenti: kiberdrošības politika, IKT resursu un informācijas sistēmu katalogs, kiberrisku pārvaldības un IKT nepārtrauktības plāns un kiberincidentu žurnāls.

Kiberdrošības politika ir paredzēta kā galvenais dokuments, kas nosaka, kā tiek organizēti subjekta kiberdrošības pasākumi. Tajā ir jābūt iekļautai tādai informācijai kā subjekta kiberdrošības pārvaldības mērķi, principi, kiberdrošības pārvaldības struktūra un nozīmīgākie kiberapdraudējumu veidi. Kiberdrošības politikas izstrāde palīdz subjektam identificēt iespējamos kiberapdraudējumus, kas var būt vērsti pret tā sistēmām, kā arī saprast prasības, kas konkrētajam subjektam ir jālevēro kiberdrošības jomā. Šis dokuments ir periodiski jāpārskata un jāaktualizē, ne retāk kā reizi trīs gados.

Minimālās kiberdrošības prasības paredz, ka subjektam jāidentificē un jāuzskaita visi tā īpašumā vai valdījumā esošie IKT resursi. Atbilstoši jauno prasību 5. pielikumā noteiktajai metodikai subjektam jānosaka konfidencialitātes, integritātes un pieejamības drošības klase (A, B vai C) katrai informācijas sistēmai un tajā elektroniski apstrādājamai informācijas resursu kategorijai (grupai). Tāpat subjektam ir jāizveido, jāuztur un jāpārskata IKT resursu un informācijas sistēmu katalogs, kā arī jānodrošina tā aktualizēšana izmaiņu gadījumā – ne vēlāk kā viena mēneša laikā. Katalogs ir jāveido atbilstoši nozarē pieņemtajai praksei, piemēram, izmantojot speciālu resursu uzskaites lietojumprogrammu. Būtiski norādīt, ka NKDC sadarbībā ar SAB ir izstrādājis vadlīnijas informācijas sistēmas drošības klases noteikšanai. Vadlīnijās ir sniegti konkrēti piemēri, kā noteikt informācijas sistēmas konfidencialitātes, integritātes un pieejamības drošības klasi un informācijas sistēmas klasi atbilstoši šo noteikumu metodikai.

Lai mazinātu potenciālos kiberdrošības riskus un nodrošinātu savlaicīgu rīcību kiberincidentu gadījumā, subjektiem atbilstoši jaunajām prasībām ir jāizstrādā un jāuztur kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns. Tas ne retāk kā reizi gadā ir jāpārskata un jāaktualizē. To var veidot kā vienu vai divus atsevišķus dokumentus. Tajā ir jābūt norādītai tādai informācijai kā, piemēram, kiberrisku novērtēšanas metodika, to novērtējums, to mazināšanas pasākumu plāns, rīcības plāns nepārtrauktības nodrošināšanai. Kiberdrošības pārvaldniekam ir jānodrošina kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izpildes kontrole.

Kontekstā ar pienākumu ziņot par notikušajiem kiberincidentiem uzņēmumam ir jālieviež arī kiberincidentu žurnāls, kurā ir jāiekļauj informācija par uzņēmuma tīklā un informācijas sistēmās konstatētājiem kiberincidentiem. Kiberdrošības žurnālā ir jānorāda tāda informācija kā kiberincidenta veids atbilstoši Minimālo kiberdrošības prasību 7. pielikumā ietvertajai tipoloģijai, kiberincidenta vispārējais apraksts, tā cēloņi un ietekmes novērtējums. Jaunās prasības paredz, ka uzņēmumam ne vēlāk kā 24 stundu laikā pēc jebkādām izmaiņām ir jāaktualizē informācija žurnālā, tādēļ, lai šo procesu atvieglotu, kiberincidentu žurnālu jau sākotnēji var veidot, piemēram, izmantojot speciālu lietojumprogrammu vai citu tehnoloģisku risinājumu.

Saskaņā ar jauno regulējumu uzņēmumiem līdztekus kiberdrošības dokumentācijas izstrādei un uzturēšanai ir pienākums ieviest vai pastiprināt arī vairākus tehniskus pasākumus, kas vērsti uz informācijas sistēmu noturības palielināšanu pret kiberuzbrukumiem un kiberincidentiem. Tas ietver, piemēram, efektīvas lietotāju piekļuves tiesību pārvaldības nodrošināšanu, kā arī regulāru rezerves kopiju izveidi visām uzņēmuma īpašumā vai valdījumā esošajām informācijas sistēmām. Vienlaikus Minimālās kiberdrošības prasības paredz papildu regulējumu arī attiecībā uz ārpakalpojumu līgumiem par IKT resursu vai pakalpojumu iegādi, stiprinot kontroli pār trešo personu iesaisti uzņēmuma digitālajā infrastruktūrā.

3. ATBILDĪGĀS IESTĀDES, SODA VEIDI

Latvijā NKDC ir noteikts par vienoto kontaktpunktu un kompetento iestādi kiberdrošības jomā, kā arī tas uzrauga kiberdrošības prasību izpildi būtisko un svarīgo pakalpojumu sniedzēju uzņēmumos un iestādēs. Centra funkcijas īsteno Aizsardzības ministrija sadarbībā ar CERT.LV. Līdztekus prasību izpildes uzraudzībai NKDC uzdevumos ietilpst arī sadarbības koordinēšana kiberdrošības jautājumos ar citu ES dalībvalstu kompetentajām iestādēm, vienotajiem kontaktpunktiem un Eiropas Komisiju, kā arī nacionālā kiberincidentu krīzes vadības plāna izstrādes nodrošināšana. Citas NKDC kompetences un tiesības ir noteiktas Kiberdrošības likumā 5. un 6. pantā.

Savukārt attiecībā uz IKT kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem uzraudzības funkcijas īsteno SAB. Tā uzdevumos ietilpst arī pārrobežu kiberincidentu risināšanas koordinēšana sadarbībā ar kiberincidentu novēršanas institūcijām. Ņemot vērā IKT kritiskās infrastruktūras stratēģisko un nacionālo nozīmi, šo infrastruktūru īpašniekiem un tiesiskajiem valdītājiem ir būtiski plašāks pienākumu un saskaņošanas procedūru loks ar SAB nekā būtisko vai svarīgo pakalpojumu sniedzējiem. Piemēram, ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai var noslēgt tikai pēc pozitīva SAB atzinuma saņemšanas.

Saskaņā ar Kiberdrošības likuma 46. pantu NKDC un SAB ir tiesības par būtisku neatbilstību Kiberdrošības likumā noteiktajām prasībām piemērot soda naudu. NKDC var piemērot soda naudu būtisko pakalpojumu sniedzējiem, bet SAB IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam – līdz 10 miljoniem eiro vai, ja to pēdējā finanšu gada kopējais neto apgrozījums pārsniedz 500 miljonus eiro, – līdz 2 % no apgrozījuma.

Savukārt svarīgo pakalpojumu sniedzējiem maksimālais sods var sasniegt 7 miljonus eiro vai, pārsniedzot 500 miljonu eiro apgrozījuma slieksni, – līdz 1,4 %, ko arī ir tiesības piemērot NKDC. Par būtisku neatbilstību likuma izpratnē uzskatāma situācija, kad subjekts nenodrošina atbilstošus kiberdrošības pasākumus, nepilda NKDC vai SAB likumīgās prasības vai savlaicīgi neziņo par nozīmīgu kiberincidentu, tostarp sniedzot nepatiesu informāciju. Kārtība, kādā nosakāms finanšu gada neto apgrozījums, no kura aprēķina soda naudu, un soda naudas apmēra noteikšanas kritēriji ir noteikti Ministru kabineta 2025. gada 29. aprīļa noteikumos

Nr. 252. Noteiktajam soda naudas apmēram ir jābūt samērīgam ar izdarīto pārkāpumu. Tomēr, ja subjekta pieļautais pārkāpums nav uzskatāms par būtisku, bet ir konstatētas neatbilstības jaunā regulējuma prasībām, NKDC vai SAB atbilstoši subjektu uzraudzības dalījumam ir tiesīgi izteikt brīdinājumu. Papildus tam iestāde var uzdot subjektam veikt konkrētas darbības neatbilstības novēršanai vai nekavējoties pārtraukt rīcību, kas pārkāpj kiberdrošības noteiktās prasībām.

Privāto tiesību juridiskajām personām ir tiesības apstrīdēt un pārsūdzēt NKDC vai SAB pieņemtos lēmumus, pieprasījumus un uzliktos tiesiskos pienākumus. NKDC lēmumus, pieprasījumus un uzliktos tiesiskos pienākumus būtisko un svarīgo pakalpojumu sniedzēji var apstrīdēt, iesniedzot iesniegumu aizsardzības ministram, savukārt aizsardzības ministra lēmums ir pārsūdzams Administratīvā procesa likumā noteiktajā kārtībā. SAB lēmumus, pieprasījumus un uzliktos tiesiskos pienākumus IKT kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji var apstrīdēt, iesniedzot iesniegumu SAB direktoram, un arī SAB direktora lēmums ir pārsūdzams Administratīvā procesa likumā noteiktajā kārtībā.

4. SECINĀJUMI – KIBERDROŠĪBA IR DIGITĀLĀS ĒRAS PAMATPRASĪBA

Lai arī jaunais regulējums paredz plašu prasību loku un tā praktiskā īstenošana prasa papildu resursus, kiberdrošības nozīme gan privātajā, gan publiskajā sektorā turpina pieaugt, ņemot vērā kiberapdraudējumu un kiberuzbrukumu skaita palielināšanos. Piemēram, 2025. gadā Apvienotās Karalistes autobūves uzņēmums "Jaguar Land Rover" piedzīvoja kiberuzbrukumu, kura rezultātā ne tikai uzņēmumam, bet arī Apvienotas Karalistes ekonomikai tika nodarīti aptuveni 2,5 miljardu ASV dolāru zaudējumi un tika skartas vairāk nekā 5000 organizācijas.[9] Savukārt Latvijā viens no pēdējā laika ievērojamākajiem kiberuzbrukumiem privātajam sektoram bija šā gada vasaras sākumā notikušais uzbrukums Jelgavas tipogrāfijai. Tās apgrozījums ir aptuveni 1,5 miljoni eiro mēnesī un apgrozījumam nodarītie zaudējumi kiberuzbrukuma rezultātā ir bijuši aptuveni 375 000 tūkstoši eiro apmērā.[10]

> PAR KIBERINCIDENTU IR UZSKATĀMS TĀDS NOTIKUMS, KAS APDRAUD UZŅĒMUMA VAI IESTĀDES APSTRĀDĀTUS DATUS VAI PAKALPOJUMA PIEEJAMĪBU, AUTENTISKUMU, INTEGRITĀTI VAI KONFIDENCIALITĀTI, KURUS PIEDĀVĀ TĪKLU UN INFORMĀCIJAS SISTĒMAS.

Nepietiekama kiberdrošības risku pārvaldība var radīt ievērojamus finansiālus zaudējumus, juridiskas sekas, tostarp strīdus par personas datu aizsardzības pārkāpumiem vai drošības prasību neievērošanu, kā arī nozīmīgu reputācijas risku uzņēmumam. Līdz ar to Kiberdrošības likuma un Minimālo kiberdrošības pienākumu izpildei ir jābūt ikviena Kiberdrošības likuma subjekta darāmo darbu augšgalā.

Ņemot vērā pieaugošo kiberapdraudējumu tendenci, uzņēmumiem un iestādēm ir ieteicams pārskatīt jaunā regulējuma prasības un iespēju robežās tās integrēt savos pārvaldības procesos. Pārdomātas kiberdrošības stratēģijas izstrāde un konsekventa īstenošana ļauj nodrošināt gan klientu datu aizsardzību, gan uzņēmuma iekšējo procesu un darbības nepārtrauktību, vienlaikus kalpojot par būtisku priekšnoteikumu reputācijas saglabāšanai un klientu uzticības stiprināšanai. Kiberdrošība ir mūsu ikviena individuālais un kolektīvais pienākums.

9 Cybersecuritydive. Jaguar Land Rover reports major earnings impact from cyberattack. Pieejams: *https://www.cybersecuritydive.com/news/jaguar-land-rover-reports-major-earnings-impact-from-cyberattack/805757/* [skatīts 15.12.202.5].

10 "Jelgavas tipogrādija" cietusi kiberuzbrukumā. Pieejams: *https://www.delfi.lv/161/criminal/120075102/jelgavas-tipografija-cietusi-kiberuzbrukuma* [skatīts 15.12.2025.].