Latvijas kiberdrošības stratēģija 2023.-2026. gadam

Struktūra

Kopsavilkums

"Latvijas kiberdrošības stratēģija 2023.–2026. gadam" (turpmāk – Stratēģija) izstrādāta, pamatojoties uz Informācijas tehnoloģiju drošības likuma 11. panta otro daļu. Tā raksturo Latvijas kiberdrošības situāciju, identificē nākotnes izaicinājumus un definē galvenos nacionālās kiberdrošības politikas rīcības virzienus laika periodam līdz 2026. gadam (ieskaitot).

Kiberdrošības politikas vīzija ir veidot drošu, atvērtu, brīvu un uzticamu Latvijas kibertelpu, kurā ir garantēta valstij un sabiedrībai nozīmīgu pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē.

Kiberdrošības politikas mērķis laika periodam no 2023. gada līdz 2026. gadam ir stiprināt Latvijas kibertelpas drošību, attīstot kiberaizsardzības spējas, paaugstinot noturību pret kiberuzbrukumiem un veicinot sabiedrības izpratni par draudiem kibertelpā, definējot šādas prioritātes: aizsardzība, atturēšana un attīstība.

Ņemot vērā Eiropas Savienības izvirzītās prioritātes un nacionālajos politikas plānošanas un citos dokumentos noteiktos mērķus, Stratēģijā izvirzīti pieci rīcības virzieni:

- Kiberdrošības pārvaldības pilnveidošana,
- Kiberdrošības veicināšana un izturētspējas stiprināšana
- Sabiedrības izpratne, izglītība un pētniecība
- Starptautiskā sadarbība un tiesiskums kibertelpā,
- Kibernoziedzības novēršana un apkarošana.

Visi iepriekšminētie rīcības virzieni ir detalizēti aprakstīti atsevišķās nodaļās, kā arī no Stratēģijas izrietošie darba uzdevumi pārskata periodam tiks apkopoti Nacionālās kiberdrošības stratēģijas uzdevumu plānā. Stratēģijā aplūkotajā laika periodā atbildīgās un iesaistītās institūcijas turpinās realizēt iepriekšējā stratēģijā iniciētos pastāvīgos uzdevumus

Atbildīgās institūcijas Stratēģijā paredzētos uzdevumus 2023. gadā īstenos piešķirto valsts budžeta līdzekļu ietvaros, savukārt jautājums par papildu valsts budžeta līdzekļu piešķiršanu 2024.–2026. gadam skatāms gadskārtējā valsts budžeta likumprojekta un vidēja termiņa budžeta ietvara likumprojekta sagatavošanas procesā kopā ar visu ministriju un citu centrālo valsts iestāžu prioritāro pasākumu pieteikumiem.

Saīsinājumi

AM	Aizsardzības ministrija
ANO	Apvienoto Nāciju Organizācija
ĀM	Ārlietu ministrija
CERT.LV	Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
CSP	Centrālā statistikas pārvalde
DDUK	Digitālās drošības uzraudzības komiteja
DVI	Datu valsts inspekcija
EĀDD	Eiropas Ārējās darbības dienests
EDSO	Eiropas Drošības un sadarbības organizācija
EM	Ekonomikas ministrija
ENISA	Eiropas Savienības Kiberdrošības aģentūra
ES	Eiropas Savienība
ESAO	Ekonomiskās sadarbības un attīstības organizācija
FM	Finanšu ministrija
IeM	Iekšlietu ministrija
IKT	Informācijas un komunikācijas tehnoloģijas
IP	Interneta protokols
IT	Informācijas tehnoloģijas
IZM	Izglītības un zinātnes ministrija
KAV	Nacionālo bruņoto spēku Zemessardzes Kiberaizsardzības vienība
KI	Kritiskā infrastruktūra
LB	Latvijas Banka
LFNA	Latvijas Finanšu nozares asociācija
LM	Labklājības ministrija
LVRTC	Latvijas Valsts radio un televīzijas centrs
MIDD	Militārās izlūkošanas un drošības dienests
MilCERT	Militāro informācijas tehnoloģiju drošības incidentu novēršanas institūcija
NATO	Ziemeļatlantijas līguma organizācija
NBS	Nacionālie bruņotie spēki
NCC-LV	Eiropas Kiberdrošības kompetenču centra Latvijas Nacionālais koordinācijas centrs
NetSafe	Latvijas Drošāka interneta centrs "Net-Safe Latvia"
NITDP[1]	Nacionālā informācijas tehnoloģiju drošības padome
NKDC	Nacionālais kiberdrošības centrs
NVO	Nevalstiskās organizācijas
SAB	Satversmes aizsardzības birojs
SM	Satiksmes ministrija
SPRK	Sabiedrisko pakalpojumu regulēšanas komisija
Stratēģija	Latvijas kiberdrošības stratēģija 2023.–2026. gadam
TM	Tieslietu ministrija
VARAM	Vides aizsardzības un reģionālās attīstības ministrija
VDD	Valsts drošības dienests
VID	Valsts ieņēmumu dienests
VIS	Valsts informācijas sistēmas
VK	Valsts kanceleja
VP	Valsts policija

[1] Likumprojektā "Nacionālās kiberdrošības likums" Nacionālās Informācijas tehnoloģiju drošības padomi tiek rosināts pārdēvēt par Nacionālās kiberdrošības Padomi. Tā kā likumprojekts vēl nav pieņemts, tad šajā dokumentā vēl tiek lietots līdzšinējais Padomes nosaukums.

Ievads

Nacionālā kiberdrošības stratēģija **definē galvenos nacionālās kiberdrošības politikas rīcības virzienus** laika periodam līdz 2026. gadam, nodrošinot "Latvijas kiberdrošības stratēģijā 2019–2022"[2] noteikto darbības virzienu pēctecību Latvijas kiberdrošības stiprināšanai, raksturo Latvijas kiberdrošības situāciju, kā arī identificē nākotnes izaicinājumus. Būtiska loma ir arī dažādu iesaistīto pušu iesaistīšana stratēģijas veidošanā un uzdevumu izpildē, veidojot drošu, atvērtu, brīvu un uzticamu Latvijas kibertelpu.

Visaptverošās valsts aizsardzības sistēmā katrai – gan valstiskai, gan nevalstiskai organizācijai, kā arī privātajam sektoram un iedzīvotājiem ir skaidri definēta loma krīzes situācijā. Arvien lielāka loma tiek piešķirta kiberdrošībai kā visaptverošās valsts aizsardzības sistēmas elementam, vēršot uzmanību ne tikai kiberdrošības pārvaldības uzlabošanai un starptautiskās sadarbības veicināšanai, bet arī sabiedrības izpratnes līmeņa celšanai. Kā šī plānošanas perioda galvenās kiberdrošības politikas prioritātes ir izvirzītas aizsardzība, atturēšana un attīstība.

Stratēģija izstrādāta sasaistē ar pārskatīto Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu Nr. 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā[3] (turpmāk – NIS2 direktīvu), kā arī ES Kiberdrošības stratēģiju digitālajai desmitgadei[4]. Izstrādājot stratēģiju, ir ņemti vērā arī nacionālie digitālās politikas plānošanas dokumentos ietvertie attīstības virzieni, ar mērķi nodrošināt saskanīgu Latvijas digitālo un kiberdrošības attīstību. Kā viens no būtiskākajiem politikas plānošanas dokumentiem šajā jomā, kas ir ņemts vērā Stratēģijas izstrādē, ir ar Ministru kabineta 2021. gada 7. jūlija rīkojumu Nr. 490 apstiprinātās "Digitālās transformācijas pamatnostādnes 2021.-2027. gadam"[5].

2023. gada pirmajā ceturksnī Ministru kabinetā tiks iesniegts konkrētu pasākumu plāns Stratēģijā izvirzīto mērķu sasniegšanai, identificējot darba uzdevumus, atbildīgās institūcijas, uzdevumu izpildes termiņus, kā arī sasniedzamos rezultātus.

---

[2] Apstiprinātas ar MK 2019. gada 17. septembra rīkojumu Nr. 40.
[3] NIS direktīva, pieejama: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016L1148.
[4] ES Kiberdrošības stratēģija digitālajai desmitgadei, pieejama: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[5] Ministru kabineta 2021. gada 7. jūlija rīkojums Nr. 490 "Par Digitālās transformācijas pamatnostādnēm 2021.–2027. gadam". https://likumi.lv/ta/id/324715

Vīzija, prioritātes un pamatprincipi

Kiberdrošības politikas vīzija ir veidot drošu, atvērtu, brīvu un uzticamu Latvijas kibertelpu, kurā ir garantēta valstij un sabiedrībai nozīmīgu pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē. Īstenojot kiberdrošības politiku, ir definētas šādas prioritātes: aizsardzība, atturēšana un attīstība.

Aizsardzība – attīstīt un pilnveidot spējas, lai aizstāvētos pret pieaugošajiem un mainīgajiem kiberdraudiem, stratēģiski plānojot IKT aizsardzību, un efektīvi reaģētu uz IKT ievainojamību ziņojumiem un drošības incidentiem, un nodrošinātu IKT aizsardzību un spēju funkcionēt. Tas ietver gan nepieciešamos tehnoloģiskos resursus, gan izpratni un zināšanas privātajam un publiskajam sektoram, kā arī sabiedrībai kopumā par iespējām sevi aizsargāt. Vienlaikus ir jānodrošina arī atbilstošs lēmumu pieņemšanas un atbildes reakcijas ātrums un izvēlēto pasākumu efektivitāte.

Atturēšana – atklāt, izmeklēt un pārtraukt ļaunprātīgas darbības kibertelpā, identificējot likumpārkāpējus un saucot pie atbildības, tādējādi atturot citus no šādu darbību veikšanas, kā arī attīstīt aktīvās kiberaizsardzības spējas.

Attīstība –attīstīt un pilnveidot publiskā sektora, būtisku pakalpojumu sniedzēju un svarīgu pakalpojumu sniedzēju IKT un IKT kritiskās infrastruktūras aizsardzību, tai skaitā, veidojot sistemātisku pieeju IKT drošības prasību uzraudzībā un kontrolē, vienlaikus veicinot izpratni un kompetenci privātajā sektorā par regulāru kiberdrošības apmācību nepieciešamību (kiberhigiēnu) un IKT drošības prasību ievērošanu.

Ņemot vērā ES izvirzītās prioritātes, nacionālajos politikas plānošanas dokumentos noteiktos mērķus, kā arī izvērtējot iepriekšējā pārskata periodā paveikto, Stratēģijā izvirzīti pieci rīcības virzieni periodam līdz 2026. gadam:

- Kiberdrošības pārvaldības pilnveidošana,
- Kiberdrošības veicināšana un izturētspējas stiprināšana
- Sabiedrības izpratne, izglītība un pētniecība
- Starptautiskā sadarbība un tiesiskums kibertelpā,
- Kibernoziedzības novēršana un apkarošana.

Kiberdrošības situācijas analīze

Situācijas raksturojums

Nacionālajā kiberdrošības stratēģijā 2019.–2022. gadam pastiprināta uzmanība tika pievērsta kiberdrošības noturībai, investīcijām IKT drošībā un personāla apmācībā. Pārskata periodā ir sperti vairāki būtiski soļi kiberdrošības veicināšanai, digitālo drošības risku mazināšanai, IKT izturētspējas, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšanai, sabiedrības izpratnes, izglītības un pētniecības izaugsmei, starptautiskās sadarbības stiprināšanai, tiesiskuma kibertelpā nodrošināšanai un kibernoziedzības mazināšanai. No pārskata periodā izvirzītā 21 uzdevuma, 19 uzdevumi jeb 90% ir izpildīti.

Līdz ar Krievijas iebrukumu Ukrainā, ir notikusi strauja reģionālās drošības situācijas pasliktināšanās, kas vēl vairāk ir aktualizējusi nepieciešamību stiprināt kiberdrošību Latvijā. Ir novērojama paaugstināta uzbrucēju aktivitāte - noris aktīva skenēšana, ievainojamību meklēšana valstiskas nozīmes sistēmās, informācijas ieguves mēģinājumi, pikšķerēšanas kampaņas, tai skaitā krāpniecisko e-pastu un sociālās inženierijas kampaņas. Lielā apjomā tiek piedzīvoti mērķēti pakalpojumatteices jeb DDoS uzbrukumi ne tikai publiskā sektora sistēmām, bet arī sabiedrībai nozīmīgu pakalpojumu sniedzēju sistēmām, kas īpaši pastiprinās līdz ar politiski vai sabiedriski nozīmīgiem notikumiem. Latvijas aktīvā loma starptautiskajā vidē un stingrā nostāja pret Krievijas agresiju Ukrainā padara to par populāru organizētu kiberuzbrukumu mērķi. Būtiskais ļaunprātīgu aktivitāšu pieaugums kibertelpā 2022. gadā norāda uz vajadzību nodrošināt gan atbilstošus personāla resursus reaģēšanai uz kiberdrošības incidentiem, gan nepieciešamību stiprināt nacionālā līmeņa spējas attīstot un pilnveidojot atbilstošus uzraudzības un kontroles mehānismus valsts funkcionēšanai nozīmīgo IKT resursu nepārtrauktības nodrošināšanai.

IKT attīstība gan Latvijā, gan ārvalstīs ir sasniegusi nebijušu ātrumu un apmēru. Jaunākās paaudzes IKT risinājumi nodrošina iespējas jebkurā laikā un vietā ātri un ērti iegūt plašu informāciju par notikumiem un procesiem Latvijā vai ārvalstīs, sazināties un apmainīties ar informāciju, veikt darījumus un norēķinus internetā, saņemt elektroniskos pakalpojumus, izveidot, parakstīt un nosūtīt elektroniskos dokumentus un saglabāt informāciju elektroniskā formā, izmantojot viedo ierīču un mākoņdatošanas pakalpojumu sniedzēju sniegtās priekšrocības.

Valsts pārvaldē daudzas no šīm tehnoloģijām tiek izmantotas un ir vitāli svarīgas sabiedrības un valsts pārvaldes iestāžu patstāvīgai un efektīvai funkcionēšanai, tādēļ ir būtiski, lai šīs tehnoloģijas būtu drošas. Kiberdrošībai tiek piešķirta aizvien lielāka nozīme, ņemot vērā sekas, kādas valstij un sabiedrībai var nodarīt pret to vērsts kiberuzbrukums. Tāpat nav noliedzams, ka kiberuzbrukumu intensitāte un sarežģītība pieaug, kas savukārt atstāj arvien lielāku ietekmi uz ikdienas dzīvi un vienlīdz apdraud gan civilo, gan militāro infrastruktūru. Turklāt kiberdraudus rada gan nevalstiskie, gan valstu aktori. Līdz ar Krievijas kara uzsākšanu Ukrainā, ir novērota tendence, ka

palielinās valstu aktoru un šo valstu darbības atbalstošo aktoru aktivitāte, ar mērķi, piemēram, ietekmēt politisko, ekonomisko vai drošības situāciju valstī, nelegāli iegūt datus vai veikt izmaiņas tajos.

Arī starptautiskajā sistēmā kopumā dažādiem kiberapdraudējumiem, līdz ar to arī kiberdrošībai, tiek pievērsta pastiprināta uzmanība. NATO sabiedroto starpā tiek stiprināta politiskā nostāja, ka arī kiberuzbrukumi konkrētos apstākļos un jo īpaši to sekas var tikt pielīdzinātas konvencionālam uzbrukumam. Atbilstoši arī ļaunprātīgas darbības kibervidē, kas rada būtiskas sekas, var kalpot par pamatu NATO 5. panta iedarbināšanai. Latvijas nacionālā kiberaizsardzības politika tiek noteikta ar tādiem valsts līmeņa plānošanas dokumentiem kā Valsts aizsardzības koncepcija[6] un atsevišķiem nozares plānošanas dokumentiem.

Tāpat arī ES dalībvalstu vidū ir vērojams visaptverošs kiberdrošības jautājumu aktualitātes un nozīmes pieaugums. Tiek prognozēts, ka šī tendence tikai pastiprināsies, sagaidāms, ka līdz 2024. gadam 22,3 miljardi ierīču visā pasaulē būs pievienotas lietu internetam.[7] Laikus reaģējot uz tendencēm kiberdrošības jomā, Eiropas Komisija un Eiropas Ārējās darbības dienests (EĀDD) 2020. gada decembrī iepazīstināja ar jauno ES Kiberdrošības stratēģiju digitālajai desmitgadei[8], kuras mērķis ir stiprināt Eiropas kopējo noturību pret kiberdraudiem un nodrošināt, lai visi iedzīvotāji un uzņēmumi varētu pilnībā izmantot priekšrocības, ko dod uzticami pakalpojumi un digitālie rīki, uz kuriem var paļauties. Lai to paveiktu, ES Kiberdrošības stratēģija paredz pārskatīt esošos un pieņemt jaunus tiesību aktus, uzliekot dalībvalstīm vairākus jaunus pienākumus kiberdrošības jomā. Vēl jo vairāk kiberdrošība tika aktualizēta kā prioritāte ES, reaģējot uz Covid-19 pandēmiju un no tās izrietošajiem izaicinājumiem un sekām attiecībā uz IKT nozari.

Jau kopš 2016. gada nozīmīga loma ir vienai no ES iniciatīvām - Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvai Nr. 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā[9] (turpmāk – NIS direktīva). Spēkā ir stājusies pārskatītā jeb NIS2 direktīva (turpmāk – NIS2 direktīva). Atšķirībā no NIS direktīvas, kas noteica drošības prasības dalībvalstu pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, pārskatītās NIS direktīvas priekšlikums iekļauj papildu sektorus: tā attieksies uz konkrētām publiskām vai privātām "būtiskām vienībām" (enerģētikas, transporta, banku pakalpojumu, finanšu tirgus infrastruktūras, veselības, dzeramā ūdens, notekūdeņu, digitālās infrastruktūras, valsts pārvaldes un kosmosa jomā) un "svarīgām vienībām" (pasta un kurjeru pakalpojumu, atkritumu apsaimniekošanas, ķīmisko vielu izgatavošanas, ražošanas un izplatīšanas, pārtikas ražošanas, pārstrādes un izplatīšanas, ražošanas un digitālo pakalpojumu sniegšanas jomā). AM kā kompetentajai iestādei

---

[6] Saeimas 2020. gada 24. septembra paziņojums "Par Valsts aizsardzības koncepcijas apstiprināšanu". https://likumi.lv/ta/id/317591

[7] ES kiberdrošības politika, pieejams: https://www.consilium.europa.eu/lv/policies/cybersecurity/.

[8] ES Kiberdrošības stratēģija, pieejama: https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52020JC0018.

[9] NIS direktīva, pieejama: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016L1148.

NIS direktīvas izpratnē ir jānodrošina, lai tiktu identificētas vienības, kas darbojas NIS2 direktīvā noteiktajās nozarēs, un lai šīs vienības veiktu atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus kiberdrošības risku pārvaldībai. Tāpat AM sadarbībā ar CERT.LV būs jāuzrauga vienībām noteikto drošības un incidentu paziņošanas prasību ievērošana, kā arī NIS2 direktīvā noteiktajā kārtībā jānosaka veicamās darbības šo prasību neievērošanas gadījumā.

Aktualitātes un nākotnes izaicinājumi

Darbaspēks

Kopīgajā paziņojumā Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot ES stipru kiberdrošību" (JOIN (2017) 450 *final*) [10], tika uzsvērts, ka līdz 2022. gadam privātajā sektorā Eiropā trūks 350 000 profesionāļu ar kiberdrošības prasmēm un šī tendence, visticamāk, turpināsies. Izaicinājums tiek radīts ne tikai tieši no kiberdrošības speciālistu trūkuma, bet arī kopējās demogrāfiskās attīstības dēļ, kas vidējā un ilgtermiņā radīs situāciju, kurā arvien mazāk cilvēku ienāks darba tirgū, nespējot nodrošināt pieprasījumu pēc noteiktu profesiju speciālistiem.

Šāds iztrūkums rada milzīgu konkurenci Eiropas un pasaules darba tirgū, kurā jākonkurē arī valsts sektoram. Latvija nav izņēmums šai tendencei, kādēļ kvalificētu speciālistu sagatavošana un piesaiste gan publiskajā, gan privātajā sektorā ir un būs būtisks izaicinājums tuvākajos gados. Kompetenta personāla trūkumam ir negatīva ietekme gan uz ikdienas darbu, gan uz spējām operatīvi reaģēt uz apdraudējumiem kibertelpā un krīzēm. Īpaši negatīva ietekme ir vērojama jautājumos, kas skar specifiskus kiberdrošības jautājumus un funkcijas, ko spēj īstenot tikai īpaši apmācīts personāls. Problēma ir sevišķi aktuāla tehniskā personāla gadījumā, kur vidējais atalgojums līdzvērtīgas kvalifikācijas un pieredzes speciālistiem privātajā sektorā ir aptuveni divas reizes lielāks par valsts un pašvaldību institūciju amatpersonu un darbinieku atlīdzības sistēmas noteikto maksimālo atalgojumu. Atbilstoši 2021. gada 16. novembrī apstiprinātajiem grozījumiem Valsts un pašvaldību iestāžu darbinieku un amatpersonu atlīdzības likumā ir iespējas pietuvināt kvalificēto ekspertu atalgojuma līmeni privātajam sektora atalgojumam, tomēr arī tas nespēj pilnībā risināt kiberdrošības speciālistu iztrūkumu. Līdz šim nav bijusi saskatāma sistemātiska pieeja kiberdrošības speciālistu sagatavošanā un, ņemot vērā šīs profesijas nenoliedzamo nākotnes potenciālu un vajadzību valstiskā līmenī, būs nepieciešams jau tuvākajā laikā meklēt risinājumu.

Jaunās ES līmeņa iniciatīvas

Kā viens no būtiskākajiem saistošajiem ES dokumentiem ir jau minētā NIS2 direktīva, kas būs pamatā lielai daļai jaunveidojamā Nacionālā kiberdrošības centra

[10] Noturība, novēršana un aizsardzība, veidojot ES kiberdrošību, pieejams: https://eur-lex.europa.eu/legal-content/lv/TXT/?uri=CELEX:52017JC0450.

(turpmāk – NKDC) uzdevumiem. Tāpat izmaiņas ieviesīs Kibernoturības akts (*Cyber Resilience Act)*[11], kura mērķis ir aizsargāt klientus un uzņēmumus no produktiem ar nedrošiem elementiem, ieviešot vienotus kiberdrošības standartus. Līdz ar kibernoturības aktu tiks ieviesti noteikumi, lai aizsargātu digitālos produktus, uz kuriem neattiecas iepriekšējo regulējumu tvērums. Kibernoturības akts būs pirmais lietu internetu jeb IoT (*Internet of Things*) regulējošais tiesību akts pasaulē. Minētās ES līmeņa iniciatīvas ir būtiskas un atbalstāmas, tomēr tās uzliks papildu birokrātisko slogu kā uzraugošajām valsts institūcijām, tā arī citiem iesaistītajiem. Kiberdrošība ir sektors, kas vēl nav pilnībā regulēts un tajā turpinās nepārtraukta attīstība, jāņem vērā, ka vidējā un ilgtermiņā darba apjoms saistībā ar dažādu ES un līdz ar to arī nacionāla līmeņa kiberdrošības prasību ieviešanu tikai palielināsies.

Informāciju sistēmu pieejamība un e-pakalpojumu saņemšana

Atbilstoši 2022. gada Valsts kontroles revīzijas ziņojumam "Vai varam paļauties uz informācijas sistēmu pieejamību un e-pakalpojumu saņemšanu" rezultātiem, ir konstatēti trūkumi informācijas sistēmu pieejamības novērtēšanā un informācijas sistēmu pārvaldībā kopumā. Ir jāveido ne tikai atbilstoša iekšējās kontroles vide un jāievieš informācijas sistēmu drošības un IKT pārvaldība, bet arī jāmēra sasniegtais rezultāts.

Valsts pārvaldes iestāžu nepietiekamais kiberdrošības līmenis

Pašreizējā situācijā bieži novērojams, ka valsts IKT projektos par kiberdrošības aspektiem tiek domāts tikai pēc CERT.LV ziņojuma saņemšanas par konstatētām problēmām vai jau notikušiem incidentiem, bet tie ir tikai atsevišķi projekti, kas nonāk CERT.LV uzmanības lokā. Problēma daļēji tika izgaismota KPMG 2019. gadā veiktajā pētījumā "Cik kiberdrošas ir Latvijas pašvaldības?".[12] Pētījuma ietvaros augsta riska līmeņa ievainojamības tika atklātas 10 no 15 novērtētajām pašvaldību tīmekļa vietnēm, savukārt visās apskatītajās pašvaldībās tika atklātas vidēja riska un zema riska līmeņa ievainojamības. Vienlaikus ir jānorāda, ka kopš 2019. gada ir mainījies gan pašvaldību skaits, gan ģeopolitiskā situācija un nav pieejamu visaptverošu pētījumu par situāciju pašvaldībās 2022. gadā. Neskatoties uz to, kopumā valsts sektorā ir nepieciešams turpināt aktīvi celt kiberdrošības līmeni. Lai valsts spētu sekot līdzi IKT straujajai attīstībai, realizēt Digitālās transformācijas pamatnostādnēs 2021.–2027. gadam noteiktos uzdevumus un mērķus, kā arī stāties pretī kiberdraudiem, valsts un pašvaldības iestādēs jānodrošina labi sakārtota un pārvaldīta IKT infrastruktūra. Tām jānodrošina IKT risinājumu un informācijas sistēmu izveide, uzturēšana un pārvaldība atbilstoši labās prakses principiem. AM kā valsts IKT drošības un aizsardzības politikas veidotāja un īstenotāja šajā jomā ir identificējusi problēmas dažādos posmos, t.i., IKT risinājumu un informācijas sistēmu plānošanas un izstrādes stadijā un pēc tam arī ieviešanas un

---

[11] Informācija par Kibernoturības aktu pieejama šeit: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[12] Cik kiberdrošas ir Latvijas pašvaldības (pētījums), pieejams: https://assets.kpmg/content/dam/kpmg/lv/pdf/2019/05/cik-kiberdro%C5%A1sas-ir-latvijas-pasvaldibas.pdf.

uzturēšanas stadijā. Ilgtermiņā ir jāveicina atbilstošu resursu piešķiršana kiberdrošības pasākumiem valsts un pašvaldību sektorā, nodrošinot finansējumu gan no iestāžu esošā budžeta, gan arī meklējot iespējas piešķirt papildu valsts budžeta finansējumu un izmantojot ES fondu sniegtās iespējas, piemēram, pašlaik tiek strādāts pie regulējuma par *Cyber Emergency Fund* jeb ātrā reaģēšanas fonda kiberdrošībai, kas varētu būt par vienu no potenciālajiem rīkiem kiberdrošības stiprināšanai kā valsts sektorā, tā privātajā sektorā.

Jauno tehnoloģiju un digitālo risinājumu droša ieviešana

Līdztekus jau esošo tehnoloģiju attīstībai, tiek piedāvātas jaunas digitālās iespējas un tiek turpināta jau esošo ieviešana, piemēram, mākslīgais intelekts, lielie dati, kvantu tehnoloģijas, 5G un nu jau arī 6G. Tas izvirza jaunas prasības tam, kā tiek aizsargāta vērtīga informācija un digitālā infrastruktūra, kas ir kritiski svarīga vitālo sabiedrības funkciju nodrošināšanai. Tas arī izvirza papildu prasības privātajam sektoram, kas ir daļa no sabiedrībai nozīmīgo pakalpojumu piegādes ķēdēm. Gan valsts sektoram, gan privātajam sektoram ir jāspēj sekot līdzi attīstībai, turklāt sagatavošanās darbi ir jāveic savlaicīgi, tostarp jānodrošina, ka tiek gatavoti arī atbilstoši jomas speciālisti.

Kiberdrošības pārvaldība

Risku pārvaldība

Ievērojot Ekonomiskās sadarbības un attīstības organizācijas (ESAO) rekomendācijas[13][14], visiem kiberdrošības pārvaldībā iesaistītajiem dalībniekiem ir jāievēro šādi četri vispārīgie kiberdrošības risku pārvaldības principi:

- Izpratne par kiberdrošības riskiem un to pārvaldību;
- Atbildības uzņemšanās par kiberdrošības risku pārvaldību;
- Kiberdrošības risku pārvarēšana pārredzamā veidā un saskaņā ar cilvēktiesībām un pamatvērtībām;
- Sadarbība, tostarp starptautiskā līmenī.

Papildu iepriekš minētajiem vispārīgajiem principiem tiek izdalīti arī četri operacionālie principi[15]:

- Risku izvērtēšanas un novēršanas cikls;

[13] ESAO rekomendācijas "Recommendation of the Council on Digital Security of Critical Activities" (2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456

[14] ESAO rekomendācijas "Digital Security Risk Management for Economic and Social Prosperity" (2015) https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf, 10 – 11.

[15] ESAO rekomendācijas "Digital Security Risk Management for Economic and Social Prosperity" (2015) https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf, 10 – 11.

- Drošības pasākumi;
- Inovācijas;
- Sagatavotība un nepārtrauktība.

Principi ņemti vērā izstrādājot Stratēģiju, vēršot uzmanību gan uz indivīda un uzņēmuma/iestādes atbildības līmeni, gan nacionālajiem un starptautiskajiem procesiem.

Pārvaldības modelis un iesaistīto dalībnieku funkcijas un pienākumi

Ministru kabinetā 2022. gada 7. jūnijā tika apstiprināts AM izstrādātais informatīvais ziņojums "Par valsts kiberdrošības pārvaldības uzlabošanu" un no 2023. gada 1. janvāra tiek uzsākta kiberdrošības pārvaldes reformas ieviešana. Reformas rezultātā kiberdrošības pārvaldība Latvijā tiks īstenota caur daļēji centralizētu pārvaldes modeli, kurā jaunveidojamais Nacionālais kiberdrošības centrs, kura darbību nodrošinās AM un CERT.LV, būs galvenā kompetentā iestāde kiberdrošības jomā un uzraudzīs NIS2 un kiberdrošības jomas nacionālo normatīvo aktu subjektus, izņemot IKT kritisko infrastruktūru, kuru tāpat kā līdz šim turpinās uzraudzīt SAB.

Valsts kiberdrošības pārvalde balstās uz savstarpēju sadarbību, kur katra valsts institūcija pilda savas funkcijas, tai skaitā kibertelpā, veicot tiešu sadarbību ar citām institūcijām un privāto sektoru vai vienotā sadarbības formātā Nacionālās informācijas tehnoloģiju drošības padomes ietvarā. Reformas ieviešanas rezultātā jaunajā kiberdrošības pārvaldības modeļa sistēmā iesaistīto dalībnieku funkcijas un pienākumi ir:

Nacionālais kiberdrošības centrs (NKDC) veido nacionālo kiberdrošības politiku un uzrauga tās īstenošanu, nodrošina NIS2 direktīvas ieviešanu un strukturētu prasību uzraudzību, nodrošina Eiropas Kiberdrošības kompetenču centra (ECCC) Latvijas Nacionālā koordinācijas centra NCC-LV darbību, kā arī atbild par kiberincidentu novēršanu un sabiedrības izglītošanu. NKDC savas kompetences ietvaros un jautājumos veido un īsteno starptautisko sadarbību.

Ārlietu ministrija (ĀM) savas kompetences ietvaros atbalsta starptautisko sadarbību un Latvijas dalību dažādās ar kiberdrošību saistītās starptautiskās iniciatīvās.

Datu valsts inspekcija (DVI) pilda Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa Regulā (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46 EK (Vispārīgā datu aizsardzības regula), Fizisko personu datu apstrādes likumā un likumā "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā" noteiktos uzdevumus personas datu apstrādes jomā.

Ekonomikas ministrija (EM) izstrādā ekonomikas politiku un veicina konkurētspējas un inovāciju attīstību.

Iekšlietu ministrija (IeM), **Valsts policija (VP)** īsteno noziedzības apkarošanas, sabiedriskās kārtības un drošības aizsardzības, personas tiesību un likumīgo interešu aizsardzības politiku. **Iekšlietu ministrijas Informācijas centrs (IC)** nodrošina tiesību sargājošo iestāžu informācijas sistēmu IKT infrastruktūras darbību.

Izglītības un zinātnes ministrija (IZM) veicina sabiedrības zināšanas un izpratni par kibertelpas zināšanu bāzes veidošanos zinātnes, tehnoloģiju, inženierijas un matemātikas jomās visos izglītības līmeņos, kā arī stiprina augstskolu pētniecības kapacitāti, nodrošinot valsts budžeta un ES struktūrfondu (Eiropas Reģionālās attīstības fonda, Eiropas Sociālā fonda) finansējumu pētniecības infrastruktūras, tajā skaitā nepieciešamā cilvēkkapitāla attīstībai un stiprināšanai.

Kultūras ministrija (KM) ir atbildīga par cilvēku medijpratības stiprināšanu formālajā un neformālajā izglītībā, sekmējot viltus ziņu un dezinformācijas atpazīšanu sabiedrībā, kā arī kritisko domāšanu.

Labklājības ministrija (LM) izstrādā un īsteno politiku darba, sociālās aizsardzības, bērnu un ģimenes tiesību, kā arī personu ar invaliditāti vienlīdzīgu iespēju un dzimumu līdztiesības jomās.

Latvijas Banka (LB) regulē un pārrauga finanšu tirgus dalībnieku darbību kibertelpā un veicina maksājumu sistēmu drošu un nepārtrauktu darbību. Savukārt kredītiestādes atbild par savas nozares elektronisko pakalpojumu drošību un pieejamību.

Latvijas Drošāka interneta centra "Net-Safe Latvia" darbību nodrošina **Latvijas Interneta asociācija (ar AM atbalstu),** izglīto sabiedrību par iespējamajiem riskiem un draudiem interneta vidē, veicina drošu interneta lietošanu un drošu interneta saturu.

Militāro izlūkošanas un drošības dienesta struktūrvienība (MilCERT) nodrošina AM un tās padotības iestāžu, tostarp Nacionālo bruņoto spēku (NBS), IKT uzraudzību. Nozares ietvaros atklāj, apstrādā informācijas tehnoloģiju drošības incidentus un koordinē to novēršanu, kā arī veic drošības pārbaudes resora informācijas sistēmu un elektronisko sakaru tīklos. MilCERT sniedz atbalstu un konsultācijas aizsardzības nozares iestāžu darbiniekiem, kuri atbild par iestāžu kiberdrošību.

NBS un Zemessardzes Kiberaizsardzības vienība (KAV) sniedz atbalstu krīzes vai apdraudējuma situācijā IT drošības incidentu novēršanā un radušos seku pārvarēšanā kibertelpā.

Nozares **nevalstiskās organizācijas** sniedz atbalstu, konsultē un sadarbojas ar NITDP kiberdrošības politikas veidošanā un īstenošanā.

Satiksmes ministrija (SM) organizē politiku elektronisko sakaru un tīklu darbības jomā.

Satversmes aizsardzības birojs (SAB) uzrauga IKT kritisko infrastruktūru.

Tieslietu ministrija (TM) izstrādā, organizē un koordinē politiku personas datu aizsardzības jomā.

Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs" (LVRTC) ir uzticamu sertifikācijas pakalpojumu sniedzējs, kurš nodrošina elektroniskās identifikācijas līdzekļu, autentifikācijas rīku, kvalificēta elektroniskā paraksta un loģiski vienotā datu centra darbībai nepieciešamo infrastruktūru, vienlaikus nodrošinot arī valsts vienotā interneta apmaiņas punkta (GLV-IX) darbību un aizsardzību pret piekļuves lieguma uzbrukumiem.

Valsts drošības dienests (VDD) ir pretizlūkošanas un iekšējās drošības dienests.

Vides aizsardzības un reģionālās attīstības ministrija (VARAM) izstrādā un koordinē politikas īstenošanu informācijas sabiedrības pārvaldībai, valsts pārvaldes pakalpojumu pārvaldībai, kā arī valsts pārvaldes digitālo tehnoloģiju pārvaldībai. Valsts reģionālās attīstības aģentūra (VRAA) nodrošina valsts IKT koplietošanas risinājumu darbību un attīstību.

Lai nodrošinātu pāreju uz daļēji centralizētu kiberdrošības pārvaldes modeli un īstenotu reformu, AM sadarbībā ar CERT.LV ir identificējusi konkrētus soļus valsts kiberdrošības pārvaldības uzlabošanai:

(1) NKDC izveide un attīstība,

(2) AM dalība valsts un pašvaldību informācijas sistēmu drošības prasību izvērtēšanā,

(3) Kompetenču centru izveide un datu centru drošības prasību gradācijas izstrāde,

(4) Drošības operāciju centru (SOC) izveide valsts institūciju informācijas sistēmu izmitināšanas datu centros,

(5) NIS2 direktīvas nacionālā ieviešana, izstrādājot un veicot grozījumus kiberdrošības jomas nacionālajos normatīvajos aktos, tai skaitā "Ministru kabineta 2015. gada 28. jūlija noteikumos Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām",

(6) NIS2 direktīvas un kibedrošības jomas nacionālo normatīvo aktu subjektu uzraudzība, atbilstoši atbildības dalījumam starp NKDC un SAB.

Nacionālās kiberdrošības politikas rīcības virzieni

Stratēģija izstrādāta sasaistē ar NIS2 direktīvu un tajā noteiktajām prasībām, ES Kiberdrošības stratēģiju digitālajai desmitgadei, Eiropas Parlamenta un Padomes 2021. gada 20. maija Regulu (ES) 2021/887, kas nosaka Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu izveidi, un Digitālas Eiropas programmas darba programmā[16] ietvertajiem kiberdrošības stiprināšanas pasākumiem, kuros skaidri iezīmēti plānotie Eiropas līmeņa pasākumi kiberdrošības jomā. Izstrādājot Stratēģiju, ir ņemti vērā arī nacionālie digitālās politikas plānošanas dokumentos ietvertie attīstības virzieni, ar mērķi nodrošināt saskanīgu Latvijas digitālo un kiberdrošības attīstību. Kā viens no būtiskākajiem politikas plānošanas dokumentiem digitālās attīstības jomā, kas ir ņemts vērā Stratēģijas izstrādē, ir ar Ministru kabineta 2021. gada 7. jūlija rīkojumu Nr. 490 apstiprinātās "Digitālās transformācijas pamatnostādnes 2021.-2027. gadam"[17].

1. rīcības virziens "Kiberdrošības pārvaldības pilnveidošana"

Rīcības virziena mērķis: Visaptverošs, efektīvs un sistemātisks kiberdrošības pārvaldības modelis, kas nodrošina NIS2 subjektu uzraudzības sistēmu ar NKDC kā vadošo iestādi

Uzdevumi:

- *Atspoguļot skaidru funkciju un atbildību sadalījumu normatīvajā bāzē*
- *Izveidot IKT koplietošanas pakalpojumu nodrošināšanas sistēmu*
- *Aktīvi iesaistīties ES saistošo tiesību aktu pilnveidē un izstrādē*
- *Integrēt ES tiesību aktu saistošās prasības nacionālajos normatīvajos aktos un procesos*
- *Stiprināt publiskā un privātā sektora sadarbību*

Kā tas ir identificēts Nacionālajā drošības koncepcijā, kiberapdraudējuma kontrole un samazināšana ir iespējama tikai sasaistē ar efektīvi īstenotu valsts kiberdrošības politiku, kas ilgtermiņā un sistemātiski nodrošinātu rīcībspēju krīzes situācijās, attīstītu informācijas un tehnoloģiju jomas tiesisko regulējumu, izglītotu sabiedrību, kā arī mērķtiecīgi strādātu pie atbildīgo institūciju spēju attīstīšanas un cilvēkresursu

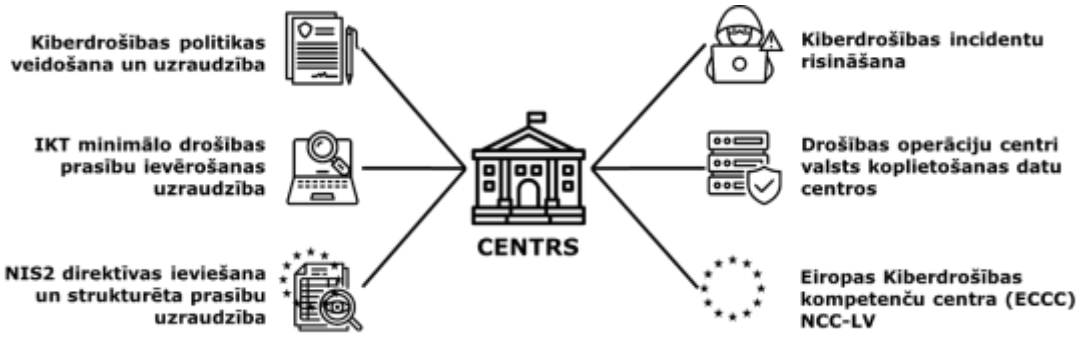
[16] Informācija par Digitālās Eiropas darba programmu: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital
[17] Ministru kabineta 2021. gada 7. jūlija rīkojums Nr. 490 "Par Digitālās transformācijas pamatnostādnēm 2021.–2027. gadam". https://likumi.lv/ta/id/324715

nodrošinājuma nozarei.[18] **Pārskata perioda galvenais mērķis kiberdrošības pārvaldības pilnveidošanas virzienā ir izveidot visaptverošu, efektīvu un sistemātisku kiberdrošības pārvaldības modeli, kas nodrošina NIS2 subjektu uzraudzības sistēmu ar NKDC un SAB kā vadošajām iestādēm.**

Līdz ar kiberdrošības nozīmes pastiprināšanos, pieaug AM un CERT.LV kiberdrošības uzdevumu apjoms un sarežģītība, tai skaitā uzdevumi no saistībām, kas izriet no ES tiesību aktiem. Vienlaikus, palielinoties nepieciešamībai stiprināt valsts kibertelpas drošību visaptverošas valsts aizsardzības ieviešanas kontekstā, tiks izveidota nacionāla kompetentā iestāde kiberdrošības jomā – NKDC, kā darbību nodrošinās AM un CERT.LV. NKDC kopīgi ar SAB veidos valsts kiberdrošības pārvaldības sistēmas kodolu.

Lai izveidotu šādu pārvaldes modeli, ir identificēti konkrēti darba virzieni. Kā viens no būtiskākajiem soļiem ir jaunā kiberdrošības pārvaldes modeļa administratīva ieviešana – 2023. gadā darbību jāuzsāk jaunajam NKDC, kas darbosies kā galvenā kompetentā iestāde kiberdrošības jomā, kurā AM veido nacionālo kiberdrošības politiku un uzrauga tās īstenošanu, savukārt CERT.LV atbild par reaģēšanu uz incidentiem, to novēršanu, sabiedrības izglītošanu un drošības operāciju centru uzraudzību (skat. shēmu). Jaunajā pārvaldes modelī tiks īstenota cieša sadarbība starp NKDC un SAB, kas uzrauga IKT kritisko infrastruktūru.

Shēma. NKDC funkcijas.



NKDC nodrošinās šādas funkcijas:

- kiberdrošības politikas veidošana (gan nacionāli, gan iesaistoties ES un NATO iniciatīvu analīzē un viedokļa paušanā) un īstenošanas uzraudzība;
- starptautiskā sadarbība kiberdrošības jomā (t.sk. Latvijas interešu pārstāvība ES un NATO kiberdrošības jautājumu darba grupās, ENISA, CyCLONe, NIS Sadarbības grupā, Eiropas Industriālo, tehnoloģisko un pētniecisko

[18] Saeimas 2019. gada 26. septembra paziņojums "Par Nacionālās drošības koncepcijas apstiprināšanu". https://likumi.lv/ta/id/309647

kiberdrošības centrā un Nacionālo koordinācijas centru tīklā, NATO CCDCOE);

- Nacionālā koordinācijas centra funkciju īstenošana, tai skaitā ECCC netieši pārvaldīto ES finanšu instrumentu vadības sistēmas izveide, ieviešana, uzraudzība un koordinācija;
- valsts pārvaldes iestāžu informācijas sistēmu izveides saskaņošana un to kiberdrošības pastāvīga izvērtēšana, rekomendāciju sniegšana kiberdrošības jautājumos, kā arī kiberdrošības prasību un NKDC rekomendāciju ieviešanas uzraudzība;
- pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju (pēc NIS2 direktīvas stāšanās spēkā – NIS2 direktīvas subjektu) uzraudzība, izņemot to subjektu uzraudzību, kuri ir IKT kritiskās infrastruktūras īpašnieki un tiesiskie valdītāji, kuiru uzraudzību arī turpmāk īstenos SAB;
- ankciju piemērošana par NKDC un SAB rekomendāciju neievērošanu;
- kiberdrošības sertifikācijas, elektroniskās identifikācijas un uzticamības pakalpojumu sniedzēju uzraudzība;
- NITDP un Digitālās drošības uzraudzības komitejas sekretariāta funkciju nodrošināšana;
- kiberdrošības incidentu novēršana;
- sabiedrības izglītošana un iesaiste;
- valsts koplietošanas datu centru, kuri nodrošina valsts datu apstrādes mākoņa darbību (turpmāk – koplietošanas datu centrs) un citu datu centru, kuros tiek uzturēti valsts IKT resursi, kā arī tajos uzturēto IKT resursu, drošības prasību gradācijas noteikšana, kā arī Kompetenču centru atbilstības noteiktajām;

Atbilstoši jaunajam pārvaldības modelim ir jāprecizē arī normatīvo aktu bāze, veidojot skaidru funkciju un atbildību sadalījumu. Būtiska ir arī IKT koplietošanas pakalpojumu nodrošināšana - jādefinē gradācijas koplietošanas datu centriem pēc to nodrošinātā drošības līmeņa un drošības operāciju centru darbības modeļi, veidojot tos koplietošanas datu centros.

Lai valsts spētu sekot līdzi IKT straujajai attīstībai, realizēt Digitālās transformācijas pamatnostādnēs 2021.–2027. gadam[19] noteiktos uzdevumus un mērķus un spētu stāties pretī kiberdraudiem, valsts un pašvaldības iestādēs jānodrošina labi sakārtota un pārvaldīta IKT infrastruktūra. Tām jānodrošina IKT risinājumu un informācijas sistēmu izveide, uzturēšana un pārvaldība atbilstoši labās prakses principiem. AM kā

[19] Digitālās transformācijas pamatnostādnes 2021.-2027. gadam, pieejamas: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam.

valsts IKT drošības un aizsardzības politikas veidotāja un īstenotāja šajā jomā ir identificējusi problēmas dažādos posmos, t.i., IKT risinājumu un informācijas sistēmu plānošanas un izstrādes stadijā un pēc tam arī ieviešanas un uzturēšanas stadijā.

Kā viena no identificētajām problēmām, ir jau IKT sistēmu plānošanas un izstrādes stadijā konstatējamas nepilnības – IKT projekti tiek realizēti, nepietiekami izvērtējot ar drošību saistītos riskus, nepārliecinoties par noteiktā drošības līmeņa atbilstību un neplānojot pietiekama apjoma drošības testus pirms sistēmu nodošanas ekspluatācijā. Sistēmu plānošanas un izstrādes stadijā iestādes koncentrējas uz pamata funkcionālajām prasībām un izmantošanas ērtībām, nepietiekamu uzmanību veltot sistēmu izvietošanas, integrācijas un drošības prasībām.

MK noteiktā kārtība[20] paredz, ka visi informācijas sistēmu attīstības projekti ir jāsaskaņo ar iesaistītajām iestādēm, tai skaitā, ar AM. Lai nodrošinātu atbilstošu AM lomu valsts un pašvaldību informācijas sistēmu drošības prasību izvērtēšanā, nepieciešams nostiprināt kārtību, ka iestādi uzraugošā ministrija kopā ar iestādi pārrunā plānoto attīstības aktivitāti, identificē sistēmas drošības riskus un citus sistēmas drošības kritērijus un vienojas par sistēmas drošības klasi atbilstoši MK noteiktajai metodoloģijai, kā arī izvērtē sagatavotā apraksta pietiekamību. Lai realizētu iepriekš minēto uzraudzības mehānismu no AM puses, pārskata periodā nepieciešams veikt izmaiņas saistošajos normatīvajos aktos.

Plānotā kārtība paredzēs, ka turpmāk jau informācijas sistēmu plānošanas un izstrādes laikā no AM puses tiktu izvērtēta valsts informācijas sistēmu noteiktā drošības līmeņa atbilstība. AM pārliecināsies, vai informācijas sistēmās paredzēts nodrošināt noteiktajam drošības līmenim atbilstošās prasības. Ieviešot šo soli, tiktu daļēji centralizēta valsts informācijas sistēmu drošības uzraudzība, tādējādi sekmējot kiberdrošību valstī un veicinot, ka tiek realizēts Latvijas Nacionālajā attīstības plānā 2021. – 2027. gadam[21] izvirzītais uzstādījums, ka ikvienam elektroniskajam pakalpojumam un risinājumam pirms ieviešanas tiks veikts kiberdrošības risku izvērtējums, vienlaikus nodrošinot kiberdrošību arī visa tā dzīvescikla laikā. Tādējādi tiks nodrošināta pakalpojuma un risinājuma nepārtrauktība, integritāte un datu aizsardzība.

Vienlaikus Latvijai kā ES dalībvalstij ir jānodrošina Savienības līmeņa saistošo dokumentu un normu integrēšana nacionālajos normatīvajos aktos un praksēs. Pārskata periodā liela uzmanība ir jāpievērš uz NIS2 direktīvas prasību ieviešanu normatīvajos aktos, nodrošinot, ka tiek izveidots NIS2 subjektu uzraudzības modelis. Šo funkciju līdz ar 2023. gadu sāks pildīt NKDC. Ņemot vērā, ka NIS2 direktīvas subjekti vienlaikus var būt arī IKT kritiskās infrastruktūras īpašnieki un tiesiskie valdītāji, kuru uzraudzību veic SAB, normatīvajos aktos tiks noteikts skaidrs uzraudzības funkciju,

---

[20] Pašreiz šo kārtību nosaka Ministru kabineta 2021. gada 31. augusta noteikumi Nr. 597 "Valsts informācijas sistēmu attīstības projektu uzraudzības kārtība", taču 2023. gadā tiks izstrādāti jauni noteikumi.

[21] Saeimas 2020. gada 2. jūlija paziņojums "Par Latvijas Nacionālo attīstības plānu 2021.–2027. gadam (NAP2027)". https://likumi.lv/ta/id/315879

tiesību un uzdevumu sadalījums starp NKDC un SAB, izveidojot vienotu uzraudzības procesu, attiecināmu, gan uz NIS2 direktīvas subjektiem, gan uz kiberdrošības jomas nacionālo normatīvo aktu subjektiem. Vienotais uzraudzības process tiks organizēts trijos līmeņos[22]:

(1) obligāts ikgadējais kiberdrošības novērtējums visiem NIS2 direktīvas subjektiem un IKT kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem;
(2) ārpuskārtas, uz risku izvērtējumu balstītas, tematiskās IKT sistēmu un resursu pārbaudes;
(3) brīvprātīga koordinētas ievainojamību atklāšanas procesa ieviešana iestādē;

IKT kritiskās infrastruktūras uzraudzību veic SAB, savukārt jaunajā kibedrošības pārvaldības modelī nepieciešamības gadījumā (piemēram, rekomendāciju vai normatīvo aktu prasību neievērošanas gadījumā) SAB varēs sniegt nepieciešamo informāciju NKDC, kas būs tiesīgs izdot IKT kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem saistošus administratīvos aktus (piemēram, uzdot novērst konstatētās neatbilstības).

Pilnvērtīga kiberdrošības pārvaldība nav iespējama bez privātā sektora iesaistes, kādēļ būtiska loma pārskata periodā ir publiskā un privātā sektora sadarbības veicināšanai. Pārskata periodā ir nepieciešams noteikt, kādi ir šīs sadarbības principi, un tos sākt ieviest praksē. Uzdevums ir veidot tādu sadarbības modeli, kas ir elastīgs, iesaistot privāto sektoru gan ilgtermiņa projektos un iniciatīvās, gan veicot operatīvas savstarpējās konsultācijas nepieciešamības gadījumos. Sadarbības modelim jābalstās divvirzienu komunikācijā pēc abpusēja izdevīguma principa, vienlaikus neveidojot liekus formālus procesus un papildu administratīvo slogu. Būtiski ir veidot attiecības, kas balstītas savstarpējā uzticībā, nodrošinot, ka notiek aktuālās informācijas aprite, valsts iestādes preventīvi informē par potenciālajiem apdraudējumiem, savukārt privātais sektors atklāti ziņo par incidentiem vai citām problēmsituācijām. Svarīgi ir uzturēt sistēmu, kurā valsts sadarbība ar privāto sektoru notiek atklātā, godīgā un nediskriminējošā veidā, pēc iespējas nodrošinot procesu un lēmumu pieņemšanas caurspīdīgumu.

[22] Plānots, ka 1. un 2. apakšpunktā minētos pasākumus attiecībā uz IKT kritisko infrastruktūru veiks SAB.

2. rīcības virziens "Kiberdrošības veicināšana un izturētspējas stiprināšana"

Rīcības virziena mērķis: Valsts pārvaldes iestādes un privātā sektora komersanti, kuru IKT resursi ir droši, pārraugāmi un atjaunojami, kā arī to darbinieki apzinās kiberdrošības riskus un spēj atbilstoši reaģēt uz apdraudējumu un incidentiem.

Uzdevumi:

- *Veicināt reāli funkcionējošu darbības nepārtrauktības plānu izveidi un testēšanu*
- *Mazināt ievainojamību, koncentrējoties uz kiberhigiēnu un drošības standartu ieviešanu*
- *Privātā sektora ietvaros veicināt izpratni par kiberdrošības standartu nepieciešamību, izvērtējot standartu pielietošanas iespējas kiberdrošības kopienas ietvaros*
- *Noteikt skaidras drošības prasības NIS2 subjektiem un ieviest nacionālo sertifikācijas modeli*
- *Izstrādāt kiberkrīžu pārvaldības plānu*
- *Nodrošināt valsts pārvaldes drošas informācijas apriti un attīstīt valsts pārvaldītus digitālās infrastruktūras stratēģiskos pakalpojumus valsts stratēģiskās autonomijas stiprināšanai*
- *Nodrošināt sabiedrību ar drošas elektroniskās saziņas valsts pārvaldītu rīku pamatkomplektu, veicināt to izmantošanas paradumus iedzīvotāju vidū*
- *Veicināt, ka jaunu valsts IS projektos un esošo projektu attīstības plānos tiek iekļautas ilgtermiņa uzturēšanas izmaksas, tostarp atbilstoša personāla piesaiste, auditēšana u.c.*
- *Izstrādāt un pastāvīgi uzturēt Eiropas Parlamenta, Saeimas un pašvaldību vēlēšanu IKT sistēmas*

Kā tas ir definēts Valsts aizsardzības koncepcijā, kiberdrošība un informācijas tehnoloģiju sistēmu noturība ir neatņemama visaptverošas valsts aizsardzības sistēmas daļa, kurā būtiska nozīme ir gan publiskajam, gan privātajam sektoram. Lai sistēma funkcionētu efektīvi, nepieciešams turpināt veikt uzlabojumus ne tikai valsts pārvaldes ietvaros, bet arī privātā sektora darbībā, tai skaitā veicinot abu sektoru ciešāku sadarbību. **Pārskata periodā par galveno mērķi ir izvirzīts uzdevums nodrošināt tādu situāciju, kurā Valsts pārvaldes iestāžu un privātā sektora komersantu IKT resursi ir droši, pārraugāmi un atjaunojami, kā arī to darbinieki apzinās kiberdrošības riskus un spēj atbilstoši reaģēt uz apdraudējumu un incidentiem.**

Lai mazinātu valsts institūciju, sabiedrības un komersantu ievainojamību kiberdrošības jomā un nodrošinātu sistēmu darbības nepārtrauktību, nepieciešams koncentrēties uz vairākiem būtiskiem aspektiem – resursu uzskaites politiku,

informācijas un informācijas sistēmu un datu kopiju veidošanas politiku, kiberdrošības apmācību (kiberhigiēnu), kā arī pašu darbības nepārtrauktības plānu izveidi un to testēšanu. Viens no kiberdrošības pārvaldes reformas soļiem daļēji centralizēta IKT pārvaldības modeļa izveidei ir IKT koplietošanas pakalpojumu nodrošināšana ar valsts datu apstrādes mākoņa palīdzību. Plānots, ka valsts datu apstrādes mākoņa attīstību un darbību nodrošinās četri koplietošanas datu centri (LVRTC, Latvijas nacionālā bibliotēka, Iekšlietu ministrijas informācijas centrs un Lauksaimniecības datu centrs). Valsts un pašvaldības iestādes varēs izmantot standartizētus valsts datu apstrādes mākoņa sniegtos pakalpojumus, tostarp dažādu līmeņu virtualizācijas un datu krātuvju pakalpojumus. No elektroniskajiem pakalpojumu katalogiem iestādes varēs izvēlēties resursus, kas tiks nodrošināti centralizēti, un ar izmitināmās informācijas sistēmas riska klasei atbilstošu resursu decentralizētas dublēšanas pakāpi. Iestādes varēs arī elektroniski noslēgt pakalpojumu līgumu. Vienlaikus iestādes varēs izvietot informācijas sistēmas arī privātajos datu centros Latvijas teritorijā, ja tiek nodrošināta atbilstība nepieciešamajiem drošības standartiem. Plānots veikt iestāžu informācijas sistēmu pārziņu izglītošanu attiecībā uz sistēmu riska novērtējumiem un nepieciešamajiem pasākumiem to ietekmes mazināšanai, ieviest valsts datu apstrādes mākoņa kritisko resursu neatkarīgu un centralizētu uzraudzību, kā arī uzturēt ciešu starpsektorālo sadarbību drošības standartu, politiku un uzturēšanas vadlīniju izstrādē, ieviešanā un ievērošanas kontrolē.

Pārskata periodā tiks precizēti atbilstošie normatīvie akti, lai skaidri noteiktu, ka valsts un pašvaldību IKT resursi tiek uzturēti koplietošanas datu centros, kas atbilst vismaz minimālajām drošības prasībām. Plānots noteikt arī skaidru gradāciju koplietošanas datu centru un citu datu centru, kur tiek uzturēti valsts un pašvaldību IKT resursi (turpmāk visi kopā – datu centri), drošības līmeņiem un tiem atbilstošām drošības prasībām, standartizējot minimālās drošības prasības. Datu centros izvietotie IKT resursi – informācijas sistēmas, reģistri, datu bāzes ir dažāda rakstura, sākot ar dokumentu un resursu vadības sistēmām un informatīvajām mājaslapām, līdz plaši izmantotiem e-pakalpojumiem, kas var kļūt par kiberuzbrukumu mērķi, vai kritiski nozīmīgiem reģistriem, kuru datu kompromitēšana var radīt plašas, reizēm neatgriezeniskas sekas.

Līdz ar datu centru izveidi, valstī nepieciešams veidot visaptverošu, centralizētu kiberdrošības stiprināšanas modeli, kas paredz CERT.LV operacionālo šūnu (*Security Operations Centre,* turpmāk – SOC) integrēšanu katrā no VARAM plānotajiem koplietošanas datu centriem. Tas koplietošanas datu centros nodrošinās mūsdienu izaicinājumiem atbilstošas apdraudējumu monitoringa, reaģēšanas, izmeklēšanas un apdraudējumu identificēšanas (*threat hunt*) spējas. SOC darbību nodrošinās NKDC. NKDC darbosies ekspertu komanda, kura uzraudzīs iestāžu datu apmaiņas plūsmu, tajā skaitā, monitorēs, analizēs un reaģēs uz drošības apdraudējumiem un uzbrukumiem, kuri vērsti pret datu centra infrastruktūru vai konkrētajām iestādēm. SOC izveidošana katrā no datu centriem ir vēl viens nepieciešams solis daļēji centralizētu valsts pārvaldes iestāžu IKT sistēmu kiberdrošības uzraudzības modeļa ieviešanai.

Katrā iestādē joprojām būtu nepieciešams IKT personāls un drošības pārvaldnieks, kuri būs atbildīgi par iestāžu infrastruktūru, kiberdrošības pasākumu plānošanu un ieviešanu, kā arī darbinieku izglītošanu kiberdrošības jomā. IKT personāls un drošības pārvaldnieki var būt arī vienoti resora ietvaros. Bet ar SOC izvietošanu datu centros, drošības pārvaldniekam iestādē nebūtu nepieciešamas padziļinātas tehniskās zināšanas drošības incidentu novēršanā, lai gan izpratne par pašiem procesiem būs nepieciešama. Tāpat arī kiberdraudu monitorēšanu, analīzi un novēršanu primāri nodrošinās SOC komanda.

Savukārt privātā sektora ietvaros būtiski ir veicināt iestāžu un uzņēmumu vadītāju līmeņa interesi un zināšanas par kiberdrošības nozīmi ne tikai krīzes situācijās, bet arī ilgtermiņā jebkuros apstākļos. Tas ietver arī papildu uzmanību tam, lai uzņēmumiem tiek nodrošināts atbalsts savstarpējai brīvprātīgai informācijas apmaiņai. Ilgtermiņa uzdevums kiberdrošības veicināšanai ir arī uzlabot, vērtēt un uzraudzīt minimālo kiberdrošības standartu ieviešanu valstī kopumā, attiecinot to gan uz valsts, gan privāto sektoru. Nodrošinot šo pirmā būtiskā soļa izpildīšanu, nepieciešams ir arī šos drošības standartus celt, veicinot, ka prasības tiek ieviestas ne tikai tādēļ, ka to nosaka normatīvie akti, bet ir arī nostiprinājusies izpratne par to nepieciešamību. Drošības standartu celšana paredz arī skaidri noteiktas iekārtas un programmatūras, kuru lietošana ir nerekomendēta vai attiecīgajiem subjektiem aizliegta. Līdz ar Eiropas Komisijas plānu IKT produktu kiberdrošības sertifikācijai, sagaidāms, ka tiks uzsākts darbs pie attiecīgo ES likumdošanas aktu izstrādes, kas savukārt noteiks papildu pienākumus dalībvalstu kompetentajām iestādēm IKT produktu kiberdrošības sertifikācijas jomā. Tas identificējams arī kā viens no pārskata perioda izaicinājumiem – nodrošināt nacionālo akreditācijas iestādes izveidi/noteikšanu, kas pildīs šo pienākumu.

Informācijas un kibertelpas aizsardzība krīzes un kara laikā jānodrošina, izmantojot aktīvos un pasīvos aizsardzības pasākumus, lai nepieļautu iedzīvotāju ārēju ietekmēšanu un rīcībspējas paralizēšanu. Lai to nodrošinātu, ir jāveicina arī valsts iestāžu sadarbība krīzes gadījumā, veidojot un izmēģinot dažādus krīzes mehānismus un procedūras. Nozīmīga loma ir arī piegāžu ķēžu drošības nodrošināšanai, pēc iespējas mazinot riskus, ka ķēdes varētu pārtrūkt krīzes apstākļos. Saistīti ir jāstiprina arī valsts sabiedrisko mediju kiberdrošība un izturētspēja, nodrošinot darbības nepārtrauktību arī krīzes apstākļos.

Lai nodrošinātu efektīvu un kiberdrošu valsts pārvaldes un pašvaldību darbību, ir nepieciešams pilnveidot un uzlabot informācijas dienesta vajadzībām drošu apriti starp publiskā sektora iestādēm. Pašlaik šādas informācijas aprite dažādās iestādēs tiek organizēta atšķirīgi, tādējādi gan potenciāli radot draudus informācijas aizsardzībai, gan apgrūtinot informācijas dienesta vajadzībām digitālu apriti publiskajā sektorā. Šīm atšķirībām ir objektīvs pamats, jo informācijas dienesta vajadzībām īpatsvars kopējā informācijas apritē dažādās institūcijās ļoti būtiski atšķiras, tādēļ atšķiras arī prakses, nepieciešamo sistēmu pieejamība un citi faktori. Neskatoties uz šīm atšķirībām, Stratēģijas pārskata periodā jāveicina droša informācijas dienesta vajadzībām aprite digitālā formā starp publiskā sektora iestādēm.

Fizisko personu identifikācijas dokumentu radīšana un izsniegšana ir viena no valsts īpaši būtiskām funkcijām, kuras pārvaldīšana un patstāvīga izpildīšana ir viena no valsts suverenitātes pazīmēm. Mūsdienu apstākļos, kad arvien lielāka daļa aktivitāšu tiek izpildītas digitālajā vidē, pieaug drošas fizisko personu elektroniskās identifikācijas nozīme. Fizisko personu elektroniskās identifikācijas likumā definējot nacionālā fizisko personu elektroniskās identifikācijas jēdzienu, šis īpaši augsta uzticamības līmeņa elektroniskās identifikācijas līdzeklis faktiski ir pielīdzināts valsts izsniegtam personas identifikācijas dokumentam digitālā vidē. Ņemot vērā elektroniskās identifikācijas risinājumu nodrošināšanas tehnoloģisko pamatu – t.i. identifikācijas līdzekļa atkarību no to nodrošinošās tehnoloģiskās platformas nepārtrauktas darbības un pieejamības, fizisko personu elektroniskās identifikācijas valsts funkcijas garantētai patstāvīgai izpildei ir nepieciešama pilna valsts kontrole ne tikai pār nacionālā elektroniskās identitātes līdzekļa izsniegšanu, bet arī pār tā darbību nodrošinošās tehnoloģiskās platformas attīstību, darbināšanu un uzturēšanu. Balstoties uz šiem apsvērumiem, tiek attīstīta un darbināta nacionālā elektroniskās identifikācijas un uzticamības pakalpojumu platforma.

Latvijas valsts attīsta un nodrošina saviem iedzīvotājiem digitālo aprīkojumu, t.sk. nacionālo elektroniskās identifikācijas līdzekli, oficiālo elektronisko adresi, kas rada iespēju digitālajā vidē droši sazināties ar valsts institūcijām un pieteikties digitālo pakalpojumu saņemšanai. Tikpat svarīga kā attiecīgo tehnoloģisko platformu radīšana un uzturēšana, ir digitālā aprīkojuma izplatīšana iedzīvotājiem un tā drošas un efektīvas lietošanas prasmju apgūšana. Mērķis, lai katra Latvijas iedzīvotāja rīcībā būtu drošs digitālais aprīkojums un prasmes to efektīvi izmantot, tiks sasniegts pakāpeniski, nostiprinot digitālā aprīkojuma izmantošanas tiesību un pienākumu regulējumu, uzlabojot digitālā aprīkojuma lietojamību un paplašinot iespējamo pielietojumu loku, kā arī veicot mērķētas komunikāciju un digitālo prasmju attīstības darbības.

Līdz ar piektās paaudzes mobilo datu pārraides tīklu izveides uzsākšanu 5G tīklu drošības garantēšana ir kļuvusi par stratēģiskās drošības jautājumu ikvienas valsts dienaskārtībā, kur jāņem vērā gan tehniskie, gan tehnoloģiskie, gan politiskie faktori. Tas arī izvirza papildu prasības privātajam sektoram, kas ir daļa no sabiedrībai nozīmīgo pakalpojumu piegādes ķēdēm. Gan valsts sektoram, gan privātajam sektoram ir jāturpina nodrošināt droša 5G tīklu ieviešana, vienlaikus savlaicīgi gatavojoties arī tālākai tehnoloģiskai attīstībai.

Brīvas un godīgas vēlēšanas ir viens no būtiskākajiem demokrātiskas valsts elementiem. Līdzīgi kā citās jomās, IKT tiek izmantotas arī vēlēšanu un to rezultātu apkopošanas procesā. Līdz ar to IKT sistēmu, kuras tiek izmantotas Eiropas Parlamenta, Saeimas un pašvaldību vēlēšanās, drošībai ir jāpievērš pastiprināta uzmanība, lai vēlēšanu godīgums netiktu apstrīdēts. Lai nodrošinātu, ka vēlēšanās izmantotās IKT sistēmas ir drošas, nepieciešams nodrošināt, ka to izstrādei un pilnveidošanai, kā arī uzturēšanai nepieciešamais finansējums ir pieejams katru gadu, nevis tikai vēlēšanu norises gadā. Šāda pieeja sniegtu iespēju konsekventi un pārdomāti

attīstīt vēlēšanu IKT sistēmas, sniedzot iespēju kompetentajām iestādēm savlaicīgi pārliecināties par to drošību. Palielinoties IKT nozīmei un izmantošanai vēlēšanās, ir jāstiprina Centrālās vēlēšanu komisijas IKT kapacitāte.

3. rīcības virziens "Sabiedrības izpratne, izglītība un pētniecība"

Rīcības virziena mērķis: Apzinātas kiberdrošības speciālistu pašreizējo apmācību iespējas un identificētas nepieciešamo nākotnes kiberdrošības speciālistu izglītības programmu vajadzības, kā arī izstrādātas fokusētas kiberdrošības informēšanas kampaņas dažādām sabiedrības grupām

Uzdevumi:

- *Apzināt esošo speciālistu kvalifikācijas celšanas vajadzības un jāveido sistēmu jaunu speciālistu izglītošanai un piesaistei*
- *Veicināt nozares profesionāļu iesaisti zināšanu apmaiņas/apmācību procesos*
- *Izveidot IS/IKT drošības pārvaldnieku apmācības/kvalifikācijas paaugstināšanas mācību programmas*
- *Identificēt un īstenot konkrētus pasākumus (informatīvās kampaņas u.c.), kas vērsti uz atsevišķām sabiedrības grupām – bērni un jaunieši, seniori, valsts pārvaldes iestāžu darbinieki, to starpā stiprināt zināšanas un izpratni par kiberhigiēnu*
- *Stiprināt kiberdrošības pētniecības attīstību Latvijā, izmantojot Digitālās Eiropas sniegtās finansējuma iespējas un veidot nepieciešamos nacionālos kiberdrošības pētniecības atbalsta mehānismus.*

Kiberdrošības politikas īstenošana gan stratēģiskā, gan tehniskā līmenī ir iespējama tikai ar kvalitatīvu kiberdrošības speciālistu piesaisti valsts pārvaldes iestādēs un privātā sektora uzņēmumos. **Pārskata perioda prioritārais mērķis ir apzināt kiberdrošības speciālistu pašreizējo apmācību iespējas un identificēt nepieciešamo nākotnes kiberdrošības speciālistu izglītības programmu vajadzības, kā arī izstrādāt fokusētas kiberdrošības informēšanas kampaņas dažādām sabiedrības grupām.**

Digitālās transformācijas pamatnostādnēs 2021.–2027. gadam[23] minēts, ka gandrīz puse no visiem Latvijas komersantiem, kas vēlas pieņemt darbā IKT jomas speciālistus, ziņo par grūtībām aizpildīt izsludinātās vakances. Līdzīgas tendences vērojamas arī Valsts kancelejas ikgadējā salīdzinošajā pētījumā par atalgojuma

[23] Digitālās transformācijas pamatnostādnes 2021.-2027. gadam, pieejamas: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam.

apmēru[24]. Pētījumā secināts, ka amatu grupa, kurā atbilstošākos kandidātus bijis gan visgrūtāk piesaistīt, gan visgrūtāk noturēt ir IKT (attiecīgi 39 % un 34 % organizāciju). Turklāt, kā liecina Ekonomikas ministrijas informatīvais ziņojums par darba tirgus vidēja un ilgtermiņa prognozēm[25], IKT speciālistu trūkums tikai turpinās pieaugt. Kvalificētu un zinošu IKT nozares speciālistu (it īpaši ar zināšanām par aktuālajiem kiberdrošības jautājumiem) trūkums skar gan AM politikas veidošanā, gan CERT.LV tehniskā līmenī. Kompetenta personāla trūkumam ir negatīva ietekme gan uz ikdienas darbu, gan uz spējām operatīvi reaģēt uz apdraudējumiem kibertelpā, kiberincidentiem un krīzēm. Īpaši negatīva ietekme ir vērojama jautājumos, kas skar specifiskus kiberdrošības jautājumus un funkcijas, ko spēj īstenot tikai īpaši apmācīts personāls. Tomēr pozitīvi jāatzīmē 2022. gadā īstenotā valsts pārvaldes atalgojuma reforma, kas ļauj nodrošināt lielāku atalgojumu kiberdrošības speciālistiem, potenciāli nodrošinot lielāku interesi par darba vietām, vienlaikus risinot tikai daļu no pastāvošās problēmas.

Lai ilgtermiņā izstrādātu plānu kiberdrošības speciālistu sagatavošanai, sākot no vidējās speciālās izglītības līdz 2. līmeņa augstākajai izglītībai, vispirms nepieciešams apzināt pašreizējās kiberdrošības speciālistu apmācības iespējas gan akadēmiskajās izglītības iestādēs, gan ārpus tās, kā arī jāizstrādā nepieciešamo nākotnes kiberdrošības speciālistu izglītības programmu vajadzības. Esošās situācijas apzināšana attiecībā pret nākotnes vajadzību, ļaus identificēt iztrūkumus piedāvājumā, ļaujot arī izglītības iestādēm veidot apmācību programmas atbilstoši tam. Būtiska ir arī profesiju standartu ieviešana, ko nepieciešams veidot atbilstoši jau esošiem starptautiskajiem standartiem. Tāpat ir jāuzsver arī KAV nozīme kvalificēta kiberdrošības personāla nodrošināšanā, sniedzot ieguldījumu gan apmācību procesā, gan personāla piesaistē, vienlaikus nodrošinot atbalstu CERT.LV un milCERT nepieciešamības gadījumā.

Iedzīvotājiem jāspēj droši rīkoties digitālajā ikdienas dzīvē, tostarp pilnvērtīgi izmantot drošas elektroniskās saziņas pamatkomplektu (eID kartes un/vai e-Paraksts *mobile* lietotne). Tas attiecas uz bērniem un jauniešiem, kā arī uz pieaugušajiem, lai pēc iespējas izvairītos no tā, ka Latvijas iedzīvotāji kļūst par kibernoziedzības vai digitālās krāpšanas upuriem. Svarīgi uzsvērt, ka tieši katra indivīda kiberhigiēnas izpratnes stiprināšana ir viens no kiberdrošības stūrakmeņiem digitālajos darba apstākļos, runājot gan par sabiedrības locekļiem kopumā, gan valsts institūciju darbiniekiem. Pilsoņiem, komersantiem un valsts iestādēm ir jāzina, kā aizsargāt sevi un būt drošām digitāli. Pārskata periodā ir jāuzlabo sabiedrības izpratne par drošu uzvedību digitālajā telpā, tai skaitā par interneta un digitālo pakalpojumu drošu lietošanu, kā arī padziļināti jāizglīto atsevišķas sabiedrības daļas par kiberdrošības jautājumiem. To starpā, uzmanība jāvērš arī uz drošo elektronisko identifikāciju un elektronisko saziņu. Lai to panāktu, nepieciešams atbalstīt Latvijas bērnu un jauniešu iesaisti starptautiskās kiberdrošības iniciatīvās, konkursos un sacensībās, nodrošinot, ka tiek veidota zināšanu bāze jau skolas vecuma bērnu vidū. Nepieciešams izstrādāt un izplatīt izglītojošus materiālus

[24] Salīdzinošs pētījums par atalgojuma apmēru, pieejams: http://petijumi.mk.gov.lv/node/3305.
[25] Informatīvais ziņojums par darba tirgus vidēja un ilgtermiņa prognozēm, pieejams: https://www.em.gov.lv/lv/darba-tirgus-zinojums.

dažādām vecuma grupām, lai pamatprasmes par drošības pasākumiem digitālās telpas un interneta lietošanā varētu apgūt un apgūtu ne tikai aktīvākie tehnoloģiju lietotāji, bet arī, piemēram, seniori. Vienlaikus tiks organizētas dažādas sociālās kampaņas par aktuālākajiem jautājumiem, piemēram, informatīva kampaņa par krāpniecības digitālajā telpā un telefonkrāpniecības riskiem. Ir nepieciešams nodrošināt aktīvu iesaisti kiberdrošības mēnesī, saistītās aktivitātes padarot par atpazīstamākajām un saistošākajām kiberdrošības jomā Latvijā. Ir arī jāveicina valsts pārvaldes institūciju zināšanu un kompetenču līmeņa celšanu, īpaši pašvaldību līmenī, veicinot darbinieku izpratni par drošu IKT lietošanu un iesaistot tos sabiedrības, valsts un pašvaldību iestāžu klientu, izglītošanā un izpratnes veidošanā par drošu saziņu ar iestādēm un iestāžu pakalpojumu saņemšanu.

Nozīmīga ir arī zinātnes un pētniecības attīstība, lai savlaicīgi gatavotos jauniem kibervides izaicinājumiem un pielāgotos tehnoloģiskajai attīstībai. Ņemot vērā Eiropas Kiberdrošības kompetenču centra un ES dalībvalstu nacionālo koordinācijas centru tīkla izveidi, Stratēģijas darbības periodā ir jāspēj identificēt prioritārie virzieni Latvijas kiberdrošības kompetenču kopienas stiprināšanai un attīstībai. Svarīgi nodrošināt, ka pieejamais ES atbalsts tiek novirzīts šo prioritāro virzienu attīstībai, tai skaitā inovatīvu kiberdrošības risinājumu ieviešanai un kiberdrošības pētniecībai. Šajā procesā centrālā loma būs Aizsardzības ministrijā izveidotajam Nacionālajam koordinācijas centram (NCC-LV), kas ir atbildīgs par kiberdrošības kompetenču kopienas izveidi un koordinēšanu, sadarbību ar citu dalībvalstu nacionālajiem koordinācijas centriem, kā arī par ES kiberdrošības atbalsta programmu ieviešanu Latvijā sadarbībā ar Centrālo finanšu un līgumu aģentūru. Būtiski ir arī veidot kompetences, lai būtu spējīgi veikt nākotnes tehnoloģiju risku un ietekmes analīzi, lai tiktu izstrādāti atbilstoši plānošanas dokumenti, attīstības scenāriji.

4. rīcības virziens "Starptautiskā sadarbība un tiesiskums kibertelpā"

Rīcības virziena mērķis: turpināt attīstīt starptautisko sadarbību, lai sekmētu starptautisko un nacionālo kiberdrošību, veicinot starptautisko normu piemērošanu kibertelpā, veidojot skaidru un uzticamu sadarbības partneru loku, kas spēj sniegt savstarpēju atbalstu kiberdraudu izvērtējumā un krīzes situācijā, ātri apmainīties ar informāciju, kā arī labajām praksēm.

Uzdevumi:

- *Stiprināt daudzpusējo un divpusējo sadarbību kiberdraudu izvērtēšanā un novēršanā, kiberincidentu atklāšanā, tostarp aktīva līdzdalība starptautiskajās mācībās un simulācijās*
- *Veicināt kibertelpas attīstību, kurā ir nodrošināta valstij un sabiedrībai nozīmīgu pakalpojumu droša sniegšana un kurā tiek ievērotas cilvēktiesības*

Pārskata perioda mērķis ir turpināt attīstīt starptautisko sadarbību, lai sekmētu starptautisko un nacionālo kiberdrošību, veicinot starptautisko normu piemērošanu kibertelpā, veidojot skaidru un uzticamu sadarbības partneru loku, kas spēj sniegt savstarpēju atbalstu kiberdraudu izvērtējumā un krīzes situācijā, ātri apmainīties ar informāciju, kā arī labajām praksēm. Jāturpina veicināt apmaiņu ar informāciju un labo praksi, sadarbību un kopēju projektu veidošanu daudzpusējos formātos, lai stiprinātu informācijas apmaiņas mehānismus un sekmētu valsts atbildīgas rīcības kibertelpā principa ievērošanu.

Kiberapdraudējumam ir pārrobežu raksturs un tas vienlaikus var būt vērsts gan pret Latvijas nacionālajām drošības interesēm, gan pret NATO, ES un Latvijas starptautiskajiem partneriem, apdraudot starptautisko un reģionālo mieru un drošību. Latvija turpinās būt aktīva dalībniece starptautiskajā cīņā pret kiberapdraudējumiem, esot uzticams partneris un atbalstot starptautiskos centienus drošas, atvērtas, brīvas un uzticamas kibertelpas veidošanai. Latvija atbalsta kibertelpu, kurā ir garantēta valstij un sabiedrībai nozīmīgu pakalpojumu droša, uzticama un nepārtraukta sniegšana un kurā tiek ievērotas cilvēktiesības.

Daudzpusējos formātos, tai skaitā ANO un EDSO, jāturpina sekmēt uzticību un drošību veicinoši pasākumi, un stingri atbalstīt principu, ka cilvēktiesību nodrošināšanai virtuālajā vidē jābūt vienlīdzīgai ar cilvēktiesību nodrošināšanu fiziskajā vidē. Jāturpina dalība ANO darba IKT drošībai[26], kopā ar līdzīgi domājošiem partneriem sekmējot esošo starptautisko normu darbību kibertelpā un iestājoties par valstu atbildīgu rīcību tajā.

[26] UN Open-ended working group on security of and in the use of information and communications technologies (OEWG).

ES formātā jāvirza likumdošanas un politikas iniciatīvas drošas un paredzamas ES kibervides attīstīšanā gan valsts institūciju darbībai, gan fiziku un juridisku personu vajadzību īstenošanai. Ar mērķi atturēt kiberuzbrukumus un kiberincidentus ES IKT sistēmām jāatbalsta ES Kiberdiplomātijas rīkkopas piemērošana, nepieciešamības gadījumā izvērtējot tās papildināšanu. ES un NATO ietvaros jāveido aktīva sadarbība un informācijas apmaiņa ekspertu darba grupās, kā arī augstāka līmeņa sanāksmēs. Jāturpina aktīva Latvijas līdzdalība kiberaizsardzības spējas stiprinošās starptautiskās mācībās un kiberuzbrukumu simulācijās, tostarp pilnveidojot NATO un ES sadarbības procedūras. Vienlaikus jāatbalsta esošo daudzpusējo un divpusējo sadarbības formātu aktīva izmantošana, rūpīgi izvērtējot jaunu formātu izveides nepieciešamību, lai nezaudētu fokusu un efektīvāk izmantotu ierobežotos resursus.

Starptautiskā sadarbība ir priekšnoteikums nopietnu kiberincidentu atklāšanai, un tā jāturpina padziļināt ar Baltijas, Ziemeļvalstu un transatlantiskajiem partneriem. Reģiona ietvaros jau ir ciešas ekonomiskās saites un reģionāla integrācija privātajā sektorā, līdz ar to nozīmīgi būtu veicināt tālāku integrāciju, kiberdraudu apzināšanā, kiberincidentu informācijas apmaiņā un citos aspektos. Viens no potenciālajiem sadarbības projektiem ir Baltijas valstu un Ziemeļvalstu reģionālā kiberdrošības operāciju centra (Security Operations Centre jeb SOC) izveide un attīstība, kas ļautu reāla laika režīmā monitorēt situāciju reģiona kibertelpā, t.sk. analizējot telemetrijas un statistikas datus, kā arī veicinātu informācijas apmaiņu starp reģiona valstu kiberincidentu novēršanas institūcijām par aktuālajiem kiberdrošības apdraudējumiem un kiberincidentiem.

Arī šajā pārskata periodā ir būtiski turpināt informācijas apmaiņu divpusējos sadarbības formātos, kas sniedz praktisku pienesumu savlaicīgai risku identificēšanai, ātrai incidentu risināšanai un sniedz iespēju labās prakses apmaiņai, ko var izmantot Latvijas kiberdrošības pārvaldības uzlabošanai.

5. rīcības virziens "Kibernoziedzības novēršana un apkarošana"

Rīcības virziena mērķis: stiprinātas Valsts policijas un valsts drošības iestāžu spējas, ieviešot jaunus un pilnā apjomā izmantojot jau esošos rīkus kibernoziedzības apkarošanai

Uzdevumi:

- *Attīstīt Valsts policijas un valsts drošības iestāžu spējas izmeklēt kiberdrošības incidentus un stiprināt šo iestāžu darbības spējas*
- *Efektīvi ieviest esošos rīkus kibernoziedzības apkarošanai pilnā apmērā un nostiprināt tos*
- *Ieviest jaunus rīkus kibernoziedzības apkarošanai – gan aktīvai iesaistei, gan preventīvām darbībām.*

Pārskata perioda mērķis ir attīstīt Valsts policijas un valsts drošības iestāžu spējas izmeklēt kibernoziedzības incidentus, kā arī stiprināt šo iestāžu darbības spējas. Kā liecina CERT.LV 2021. gadā veiktā iedzīvotāju aptauja, vairāk nekā 70% aptaujāto Latvijas iedzīvotāju maldīgi uzskata, ka nav pakļauti kiberuzbrukuma riskam. Patiesībā šādam riskam pakļauts ir ikviens Latvijas iedzīvotājs, par to liecina arī Valsts policijas kopš 2017. gada apkopotā statistika par iedzīvotāju zaudējumiem dažādās starptautiskās krāpniecību shēmās interneta vidē – vismaz 1500 cietušajiem izkrāpti kopsummā vairāk nekā 14,5 miljoni eiro**.** Šī statistika ir tikai par zināmajiem gadījumiem, realitātē summu apjoms varētu būt vēl lielāks, jo ne visi cietušie ziņo tiesībsargājošām iestādēm. Ņemot vērā iepriekš minēto, ir jāveicina sabiedrības izpratne par kibertelpu un kibernoziegumu riskiem tajā, lai stiprinātu Latvijas sabiedrības noturību pret kiberzubrukumiem, mazinātu to ietekmi un sekmētu to novēršanu.

Cīnoties ar kibernoziedzību, nepieciešama esošo rīku nostiprināšana un paplašināšana, ieviešot arī jaunus rīkus kibernoziedzības novēršanai. Jāvērš uzmanība ne tikai uz informācijas sniegšanu, atvieglojot veidu, kādā iedzīvotājiem ir iespēja ziņot par iespējamiem noziedzīgiem nodarījumiem, kas potenciāli ļautu palielināt ziņu sniedzēju aktivitāti, bet arī uz ātru saņemtās informācijas apstrādi, šķirošanu, mērķētu virzīšanu un atbildes sniegšanu, lai informācijas aprite būtu pēc iespējas efektīva. Savukārt, palielinoties ziņu sniedzēju aktivitātei, vienlaikus būs nepieciešams palielināt Valsts policijas un drošības iestāžu resursus. Tādējādi būtiska ir kvalificētu speciālistu piesaiste un atbalsts, zināšanu pilnveide un starptautiskās sadarbības veicināšana kibernoziegumu izmeklēšanā un prevencijā, lai Valsts policija savlaicīgi novērstu, atklātu un pārtrauktu to izdarīšanu, un sauktu vainīgos pie krimināltatbildības.

Īpaša uzmanība ir jāpievērš preventīvām metodēm un iniciatīvām, kas ļautu bloķēt ar noziedzīgu mērķi radītām vai noziedzīgām darbībām izmantotas interneta vietnes, šo iniciatīvu atzīšanu un iedzīvināšanu, pilnveidojot arī iesaistīto institūciju sadarbību un atbildīgo institūciju reaģēšanas ātrumu.

Finansiālās ietekmes novērtējums

Stratēģijas īstenošanai plānotie finanšu avoti ir valsts un pašvaldību budžets. Rīcības virzienu uzdevumu īstenošanai var piesaistīt ES struktūrfondu (Eiropas Reģionālās attīstības fonds, Eiropas Sociālais fonds, Kohēzijas fonds) finanšu līdzekļus. Tāpat ir iespējams piesaistīt ES finanšu instrumentu "Digitālā Eiropa" un "Apvārsnis Eiropa" apakšprogrammu ietvaros kiberdrošības jomā īstenojamo projektu finansējumu. Stratēģijā noteikto rīcības virzienu finansēšanai var tikt piesaistīts arī privātais kapitāls, kas iespējams, veiksmīgi attīstot publiskās un privātās partnerattiecības, kā arī citus risinājumus privātā kapitāla piesaistei. Stratēģijā paredzēto uzdevumu īstenošana 2023. – 2026[27]. gadam tiks nodrošināta Stratēģijā minētajām atbildīgām institūcijām piešķirto valsts budžeta līdzekļu ietvaros.

1. tabula

Kopsavilkums par Stratēģijā iekļauto rīcības virzienu īstenošanai piešķirto finansējumu pa gadiem Aizsardzības ministrijas budžeta ietvaros (EUR)*

Rīcības virziens	2023. gads	2024. gads	2025. gads	2026. gads un turpmāk	Kopā
1. Kiberdrošības pārvaldības pilnveidošana	4 031 872	5 210 269	5 611 654	5 611 654	20 465 449[28] (nepārsniedzot)
2. Kiberdrošības veicināšana un izturētspējas stiprināšana[29]	0	0	0	0	**0**
3. Sabiedrības izpratne, izglītība un pētniecība	0	0	0	0	**0**

[27] Jautājums par papildu valsts budžeta līdzekļu piešķiršanu 2024.–2026. gadam skatāms likumprojekta par valsts budžetu kārtējam gadam un vidēja termiņa budžeta ietvaru sagatavošanas procesā kopā ar visu ministriju un citu centrālo valsts iestāžu prioritāro pasākumu pieteikumiem.

[28] Ar Nacionālā kiberdrošības centra izveidi saistītās papildu personāla izmaksas atbilstoši Aizsardzības ministrijas informatīvajam ziņojumam "Par valsts kiberdrošības pārvaldības uzlabošanu" (Apstiprināts ar Ministru kabineta 07.06.2022. sēdes protokolu Nr.30/4§). Aprēķinos nav iekļautas Aizsardzības ministrijas un CERT.LV darba vietu iekārtošanas, uzturēšanas un citas saistītās papildu izmaksas.

[29] Šajā rīcības virzienā plānoto SOC veidošanai šobrīd ir paredzēts finansējums SOC personāla nodrošināšanai, kas ir iekļauts kopējā finansējumā rīcības virziena "Kiberdrošības pārvaldības stiprināšana" īstenošanai. Savukārt detalizētas izmaksas SOC izveidei vēl tiks aprēķinātas, un SOC projekta finansējums plānošanas un sākotnējās ieviešanas stadijā stratēģijas darbības periodā no 2023. līdz 2026. gadam tiks nodrošināts Aizsardzības ministrijai piešķirto valsts budžeta līdzekļu ietvaros.

Rīcības virziens	2023. gads	2024. gads	2025. gads	2026. gads un turpmāk	Kopā
4. Starptautiskā sadarbība un tiesiskums kibertelpā	0	0	0	0	**0**
5. Kibernoziedzības novēršana un apkarošana	0	0	0	0	**0**
Kopā	**4 031 872**	**5 210 269**	**5 611 654**	**5 611 654**	**20 465 449**

*Ir identificēts arī finansējuma apjoms vairākiem projektiem, taču tā apjoms un sadalījums pa gadiem ir informācija dienesta vajadzībām, kādēļ netiek iekļauta šajā pārskata tabulā.

Stratēģijas ieviešanas izvērtējums

Izvērtējuma metodoloģija

Lai nodrošinātu stratēģijā izvirzīto mērķu un prioritāšu īstenošanu, nepieciešams izveidot regulāru stratēģijas ieviešanas novērtējuma mehānismu. Paredzēts, ka divas reizes gadā Nacionālās IT drošības padomes ietvaros tiek izskatīts esošais uzdevumu statuss, veikta to aktualizācija, kā arī apspriesti risinājumi, ja ir identificēti kavēkļi savlaicīgai uzdevumu izpildei.

Progresa noteikšanai tiks ņemts vērā kiberdrošības brieduma līmeņa izvērtējums, kam par pamatu tiks izmantots ENISA līmeņu iedalījums, veicot pašnovērtējumu.

Pārskatu iesniegšanas kārtība

Aizsardzības ministrija sadarbībā ar visām iesaistītajām institūcijām un NITDP līdz 2026. gada 1. maijam iesniedz Ministru kabinetā informatīvo ziņojumu par Stratēģijas uzdevumu īstenošanas novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem.

Noslēguma jautājumi

Piedāvātā risinājuma sākotnējais (*ex-ante*) ietekmes novērtējums nav veikts, jo kiberdrošība pastāvīgi un strauji evolucionē, bet Stratēģijā noteiktie rīcības virzieni ir

Nacionālās drošības koncepcijā iepriekš noteikto prioritāšu un līdz šim uzsākto darbību turpinājums.

Nav tādu politikas plānošanas dokumentu, kuri būtu atzīstami par spēku zaudējušiem.