Informatīvais ziņojums

**“Par pamatnostādņu “Latvijas kiberdrošības stratēģija 2014.–2018. gadam” rīcības plāna īstenošanu”**

Rīga

2019

**Saturs**

[Ievads 3](#_Toc10448062)

[Saīsinājumi 4](#_Toc10448063)

[1. Situācijas raksturojums 6](#_Toc10448064)

[2. Stratēģijas rīcības virzienu uzdevumu izpilde 7](#_Toc10448065)

[2.1. Kiberdrošības pārvaldība un resursi 7](#_Toc10448066)

[2.2. Tiesiskums kibertelpā un kibernoziedzības mazināšana 8](#_Toc10448067)

[2.3. Sagatavotība un rīcībspēja krīzes situācijā 8](#_Toc10448068)

[2.4. Sabiedrības izpratne, izglītība un pētniecība 9](#_Toc10448069)

[2.5. Starptautiskā sadarbība 10](#_Toc10448070)

[2.6. Kopsavilkums par stratēģijas rīcības virzienu uzdevumu izpildes statusu 11](#_Toc10448071)

[3. Priekšlikumi kiberdrošības politikas jomā turpmākajiem gadiem 11](#_Toc10448072)

[4. Secinājumi 12](#_Toc10448073)

1. pielikums

2. pielikums (DIENESTA VAJADZĪBĀM)

# **Ievads**

Pamatnostādnes “Latvijas kiberdrošības stratēģija 2014.–2018. gadam” (turpmāk – stratēģija) tika apstiprinātas ar Ministru kabineta (turpmāk – MK) 2014. gada 21. janvāra rīkojumu Nr. 40 “Par pamatnostādnēm “Latvijas kiberdrošības stratēģija 2014.-2018. gadam”. Turpmākās rīcības plānojums ar 68 kiberdrošības stratēģijas mērķu sasniegšanas uzdevumiem un attiecīgu atbildības sadalījumu (turpmāk – rīcības plāns) tika pievienots stratēģijai kā 2. pielikums (vispārējas pieejamības informācija) un 3. pielikums (informācija dienesta vajadzībām), apstiprinot šos grozījumus ar MK 2014. gada 9. jūlija rīkojumu Nr. 347 “Grozījumi pamatnostādnēs “Latvijas kiberdrošības stratēģija 2014.-2018. gadam”.

Stratēģijas grozījumi paredz, ka AM sadarbībā ar visām iesaistītajām ministrijām un NITDP līdz 2016. gada 1. februārim jāiesniedz MK informatīvais ziņojums par pamatnostādņu rīcības plānā noteikto uzdevumu ieviešanas gaitu, bet līdz 2019. gada 1. jūnijam – informatīvais ziņojums par pamatnostādņu rīcības plāna īstenošanas galīgo novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem. Izpildot iepriekšminēto, AM iesniedza MK informatīvo ziņojumu par pamatnostādņu rīcības plānā noteikto uzdevumu ieviešanas gaitu, kuru izskatīja Ministru kabineta 2016. gada 29. marta sēdē.

Informatīvā ziņojuma “Par pamatnostādņu “Latvijas kiberdrošības stratēģija 2014.–2018. gadam” rīcības plāna īstenošanu” (turpmāk – informatīvais ziņojums) sagatavošanā tika iesaistītas visas stratēģijas rīcības plānā noteiktās, par uzdevumu izpildi atbildīgās institūcijas, kuru sniegtā informācija tika izmantota informatīvā ziņojuma sagatavošanā. Jautājums par rīcības plāna īstenošanas galīgo novērtējumu tika skatīts NITDP 2019. gada 15. maija sēdē.

Informatīvais ziņojums ir strukturēts vairākās nodaļās. Informatīvā ziņojuma sākumā ir atšifrēti saīsinājumi, savukārt pirmajā nodaļā ir sniegts situācijas apraksts stratēģijas pārskata periodā – no 2014. līdz 2018. gada beigām. Otrajā nodaļā sniegts kopsavilkums par visu piecu stratēģijas rīcības virzienu uzdevumu izpildes statusu. Trešajā nodaļā ir aplūkoti priekšlikumi kiberdrošības politikas jomā turpmākajiem gadiem, tai seko ceturtā nodaļa – secinājumi. Informatīvajam ziņojumam ir divi pielikumi. 1. pielikumā ir pieejams pārskats par stratēģijas 2. pielikuma uzdevumu izpildes statusu, savukārt 2. pielikumā – pārskats par stratēģijas 3. pielikuma uzdevumu izpildi. Tā kā stratēģijas 3. pielikumam ir noteikts statuss “Dienesta vajadzībām”, arī informatīvā ziņojuma 2. pielikumam ir tāds pats informācijas pieejamības ierobežojuma statuss.

# **Saīsinājumi**

ABS Agrās brīdināšanas sistēma

ADAS Automatizētas datu apstrādes sistēmas

AIP Augstākās izglītības padome

ANO Apvienoto Nāciju Organizācija

AM Aizsardzības ministrija

ĀM Ārlietu ministrija

ĀSVEST Ārkārtas situāciju valsts elektronisko sakaru tīkls

CCDCOE NATO Informācijas tehnoloģiju aizsardzības izcilības centrs Tallinā

CERT.LV Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

DVI Datu valsts inspekcija

DP Drošības policija

EEZ Eiropas Ekonomiskā zona

EDSO Eiropas Drošības un sadarbības organizācija

eID Elektroniskās identifikācijas karte

EK Eiropas Komisija

EM Ekonomikas ministrija

ENISA Eiropas Tīklu un informācijas drošības aģentūra

ERAF Eiropas Reģionālās attīstības fonds

ES Eiropas Savienība

ESF Eiropas Sociālais fonds

EUCOM ASV Bruņoto spēku Eiropas virspavēlniecība

FKTK Finanšu un kapitāla tirgus komisija

GKrPP ENAP Galvenās kriminālpolicijas pārvaldes Ekonomisko noziegumu apkarošanas pārvalde

ĢP Ģenerālprokuratūra

IeM Iekšlietu ministrija

IeM IC Iekšlietu ministrijas Informācijas centrs

IKT Informācijas un komunikācijas tehnoloģijas

ISACA Biedrība “ISACA Latvijas nodaļa”

IT Informācijas tehnoloģijas

IZM Izglītības un zinātnes ministrija

JPI Jaunās politikas iniciatīva

KAV Nacionālo bruņoto spēku Kiberaizsardzības vienība

LB Latvijas Banka

LDDK Latvijas Darba devēju konfederācija

LIA Latvijas Interneta asociācija

LIKTA Latvijas Informācijas un komunikācijas tehnoloģijas asociācija

LKA Latvijas Komercbanku asociācija

LM Labklājības ministrija

LPESPS Latvijas prezidentūras Eiropas Savienības Padomē sekretariāts

LPMC Latvijas Pašvaldību mācību centrs

LTRK Latvijas Tirdzniecības un rūpniecības kamera

LU Latvijas Universitāte

LU MII Latvijas Universitātes Matemātikas un informātikas institūts

LVDC Loģiski vienotais datu centrs

LVRTC Latvijas Valsts radio un televīzijas centrs

LZA TK Latvijas Zinātņu akadēmijas Terminoloģijas komisija

MIDD Militārās izlūkošanas un drošības dienests

MilCERT Militāro informācijas tehnoloģiju drošības incidentu novēršanas komanda

MK Ministru kabinets

NAP Nacionālais attīstības plāns

NATO Ziemeļatlantijas līguma organizācija

NBS Nacionālie bruņotie spēki

NetSafe Latvijas Drošāka interneta centrs “Net-Safe Latvia”

NEVIS [Novērtēšanas elektroniskās veidlapas informācijas](https://nevis.mk.gov.lv/UI/Default.aspx) sistēma

NITDP Nacionālā informācijas tehnoloģiju drošības padome

NVO Nevalstiskās organizācijas

PMLP Pilsonības un migrācijas lietu pārvalde

PVN Pievienotās vērtības nodoklis

SAB Satversmes aizsardzības birojs

SIA Sabiedrības ar ierobežotu atbildību

SM Satiksmes ministrija

SPRK Sabiedrisko pakalpojumu regulēšanas komisija

TM Tieslietu ministrija

VARAM Vides aizsardzības un reģionālās attīstības ministrija

VBTAI Valsts bērnu tiesību aizsardzības inspekcija

VDAR Vispārīgās datu aizsardzības regula

VDD Valsts drošības dienests

VESPC Valsts elektronisko sakaru pakalpojumu centrs

VIS Valsts informācijas sistēmas

VISC Valsts izglītības satura centrs

VK Valsts kanceleja

VP Valsts policija

VRAA Valsts reģionālās attīstības aģentūra

VVC Valsts valodas centrs

# **Situācijas raksturojums**

Stratēģijas pārskata periodā tika veiktas izmaiņas kiberdrošības jomu regulējošajos normatīvajos aktos. 2015. gada 5. februārī tika apstiprināti grozījumi Informācijas tehnoloģiju drošības likumā, papildinot likumu ar jaunu punktu, nosakot, kā institūcijām ir jārīkojas informācijas tehnoloģiju drošības nepilnību gadījumā. Uz minēto grozījumu pamata tika izstrādāti MK 2015. gada 28. jūlija noteikumi Nr. 422 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”, kuru mērķis ir stiprināt valsts un pašvaldību IKT resursu drošību, nosakot minimālās drošības prasības.

Informācijas tehnoloģiju drošības likumā tika izdarīti grozījumi arī 2017. gada 15. jūnijā, pirmkārt, lai precizētu LU MII nosaukumu, otrkārt, nodotu MIDD uzdevumus un tiesības, kurus uz deleģējuma līguma pamata veica LU MII struktūrvienība – Informācijas tehnoloģiju drošības incidentu novēršanas institūcija attiecībā uz AM un tās padotībā esošajām iestādēm un NBS IKT, un, treškārt, CERT.LV vai MIDD būtu tiesības pieprasīt atslēgt “.lv” domēna vārdu, ja tas iesaistīts drošības incidentā.

Latvijas tiesību aktos ir pārņemtas Eiropas Parlamenta un (Eiropas) Padomes 2016. gada 6. jūlija direktīvā (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā noteiktās prasības. Ir ieviesti jauni tiesību subjekti – pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, kuriem ir noteikts pienākums ziņot par informācijas tehnoloģiju drošības incidentiem, kuri būtiski ietekmē pakalpojumu sniedzēju pamatpakalpojumu vai digitālo pakalpojumu, un ievērot konkrētas informācijas sistēmu drošības prasības.

2019. gada 18. janvārī MK noteikumos Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” spēkā stājās norma, kas paredz, ka valsts un pašvaldību institūcijas ievēro kompetentās valsts drošības iestādes un Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas izstrādātos ieteikumus par izmantojamām informācijas un komunikācijas tehnoloģijām (tostarp par bezmaksas programmatūru un veicamajiem drošības pasākumiem).

2015. gada 4. novembrī Latvijas Republikas Aizsardzības ministrija, Igaunijas Ekonomikas jautājumu un komunikācijas ministrija un Lietuvas Nacionālās aizsardzības ministrija (par kiberdrošību atbildīgās institūcijas) parakstīja saprašanās memorandu par sadarbību kiberdrošības jomā. Kiberdrošības jautājumi tiek regulāri apspriesti Baltijas valstu, NB8 un starpvalstu sanāksmju formātos. CERT.LV sadarbojas ar Igaunijas (Informācijas sistēmu pārvalde, RIA) un Lietuvas (Nacionālais kiberdrošības centrs, NCSC) informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

Kompetentās iestādes Latvijā, kuras nodrošina efektīvu reaģētspēju un atbalstu kiberuzbrukumu skartajām iestādēm, ir CERT.LV, MilCERT (izveidots 2016. gadā) un KAV (izveidota 2013. gadā). Vienlaikus būtiska loma Latvijas kiberdrošības politikas koordinēšanā ir NITDP, kuras mērķis ir koordinēt ar informācijas tehnoloģiju drošību saistītās politikas izstrādi, kā arī attiecīgu uzdevumu un pasākumu plānošanu un īstenošanu.

Saskaņā ar CERT.LV ceturkšņu pārskatos sniegto informāciju pēdējos divos gados kiberuzbrukumu intensitātes līmenis ir stabils, ar nelieliem kāpumiem. Ilgtermiņā kiberuzbrukumu skaitam ir tendence pieaugt. 2018. gadā vairāk nekā 2017. gadā tika novēroti ielaušanās un informācijas vākšanas mēģinājumi, kas varētu būt saistīts ar Saeimas vēlēšanām 2018. gada rudenī.

Vēlēšanu raksturs padara tās neaizsargātas no daudziem drošības apdraudējumiem, kas vērsti pret to dalībniekiem, infrastruktūru un informāciju. Pirms 2018. gada 6. oktobra Saeimas vēlēšanām tika izveidota koordinācijas grupa, lai novērstu maldinošas informācijas kampaņas masu informācijas līdzekļos. Grupa turpina darbu arī pirms Eiropas Parlamenta vēlēšanām, jo ES līmenī ir atzīti riski vēlēšanu drošībai. Eiropas Parlaments, ES dalībvalstis, EK un ENISA 2019. gada 5. aprīlī organizēja pasākumu, lai pārbaudītu ES reakciju un krīzes plānus iespējamiem kiberdrošības negadījumiem, kas ietekmē ES vēlēšanas. Mācību mērķis bija pārbaudīt, cik efektīvas ir ES dalībvalstis un ES reaģēšanas prakse un krīzes plāni, un noteikt veidus, kā novērst, atklāt un mazināt kiberdrošības incidentus, kas var ietekmēt gaidāmās ES vēlēšanas.

# **Stratēģijas rīcības virzienu uzdevumu izpilde**

Informatīvā ziņojuma otrā nodaļa sniedz kopsavilkumu par visu piecu stratēģijas rīcības plāna virzienu uzdevumu izpildes statusu. Aprakstu par katra uzdevuma vai pasākuma izpildi un tās gaitā konstatētajiem izaicinājumiem lūdzu skatīt informatīvā ziņojuma 1. un 2. pielikumā (DIENESTA VAJADZĪBĀM).

## **Kiberdrošības pārvaldība un resursi**

Rīcības virzienam “Kiberdrošības pārvaldības un resursi” ir 3 apakšvirzieni un 27 uzdevumi, pieciem no tiem ir statuss “Informācija dienesta vajadzībām”. Informāciju par 1. rīcības virziena 22 uzdevumu izpildes statusu skatīt 1. shēmā.

*1. shēma* 1. rīcības virziena uzdevumu izpildes statuss

Četrpadsmit (14) uzdevumi, kas veido 64% no visiem rīcības virziena “Kiberdrošības pārvaldības un resursi” uzdevumiem, neskaitot uzdevumus ar statusu “Informācija dienesta vajadzībām”, ir izpildīti, savukārt par 1 uzdevuma izpildes statusu informācija nav saņemta. Par šī uzdevuma izpildi atbildīgā institūcija ir AIP (1.19. uzdevums).

Izvērtējuma par nepieciešamību pilnveidot esošos elektronisko sakaru maģistrālos tīklus izstrāde ir zaudējusi aktualitāti. Turklāt vairākiem uzdevumiem – esošās elektronisko sakaru tīklu infrastruktūras kartēšanai, publiskās pārvaldes informācijas sistēmu risku novērtējumam un analīzei, Latvijas centralizētās IKT drošības un profilakses platformas izveidei, valsts IKT drošības pārvaldības pasākumu atskaitīšanās mehānisma izveidei, valsts pārvaldes iestāžu informēšanai par nepieciešamību nodrošināt personas datu apstrādes drošību interneta vidē, izvērtējumam un tiesību aktu pilnveidei saistībā ar minimālajām kompetencēm atbildīgajām personām, pašnovērtējuma kompetenču vadlīnijām, kuru rezultātā iespējams konsolidēt mācību vajadzības – netika piešķirts finansējums. Tomēr 1.21. un 1.22. uzdevums ir izpildīts, citi finansējuma dēļ ir izpildes procesā, daļēji izpildīti, nav izpildīti vai arī nav uzsākti.

## **Tiesiskums kibertelpā un kibernoziedzības mazināšana**

Rīcības virzienā “Tiesiskums kibertelpā un kibernoziedzības mazināšana” ir 8 uzdevumi. Informāciju par 2. rīcības virziena 8 uzdevumu izpildes statusu skatīt 2. shēmā.

*2. shēma.* 2. rīcības virziena uzdevumu izpildes statuss

Seši (6) uzdevumi, kas veido 75% no visiem rīcības virziena “Tiesiskums kibertelpā un kibernoziedzības mazināšana” uzdevumiem, ir izpildīti.

Kiberdrošībā lietoto terminu definīciju izstrāde latviešu valodā nav izpildīta. Uzdevuma izpilde netika uzsākta, jo uzdevumam netika piešķirts finansējums. Uzraudzībai, lai IS pārziņi savās darbībās ar personas datiem ieviestu un nodrošinātu augsta līmeņa aizsardzības pasākumus, netika piešķirts finansējums, līdz ar to DVI uzraudzību īstenoja esošā budžeta ietvaros, nodrošinot VDAR paredzēto prasību attiecībā uz personas datu apstrādes uzraudzību īstenošanu, ietverot konkrētos uzraudzības pasākumus visaptverošā personas datu apstrādes uzraudzības mehānismā. Uzdevums ir izpildes procesā.

## **Sagatavotība un rīcībspēja krīzes situācijā**

Rīcības virzienā “Sagatavotība un rīcībspēja krīzes situācijā” ir 15 uzdevumi, četriem no tiem ir statuss “Informācija dienesta vajadzībām”. Informāciju par 3. rīcības virziena 11 uzdevumu izpildes statusu skatīt 3. shēmā.

Astoņi (8) uzdevumi, kas veido 73% no visiem rīcības virziena “Sagatavotība un rīcībspēja krīzes situācijā” uzdevumiem, neskaitot uzdevumus ar statusu “Informācija dienesta vajadzībām”, ir izpildīti.

Iekšlietu ministrijas Rezerves datu centra risinājuma izveide ir izpildes procesā. Projekta “Loģiski vienotais datu centrs”, kura ietvaros ir paredzēts īstenot šo uzdevumu, detalizēts apraksts ir saskaņots un tā iekļaušana valsts vienotajā IKT mērķarhitektūrā ir apstiprināta ar MK 2017. gada 9. augusta rīkojumu Nr. 420 “Par informācijas sabiedrības attīstības pamatnostādņu ieviešanu publiskās pārvaldes informācijas sistēmu jomā (mērķarhitektūras 12.0. versija)”.

*3. shēma*. 3. rīcības virziena uzdevumu izpildes statuss

Nacionālā virtuālā, ārējā perimetra stiprināšanas izvērtējums ir zaudējis aktualitāti, taču SM ir iesniegusi jaunu priekšlikumu un jaunais uzdevums ir iekļauts informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projektā. Savukārt satelīta datu pārraides risinājums starp ĀM centrālo aparātu un Pastāvīgo pārstāvniecību ES ir izpildes procesā – tā izpildes termiņš ir 2020. gada 4. ceturksnis.

## **Sabiedrības izpratne, izglītība un pētniecība**

Rīcības virzienā “Sabiedrības izpratne, izglītība un pētniecība” ir 9 uzdevumi. Informāciju par 4. rīcības virziena 9 uzdevumu izpildes statusu skatīt 4. shēmā.

*4. shēma*. 4. rīcības virziena uzdevumu izpildes statuss

Seši (6) uzdevumi, kas veido 67% no viesiem rīcības virziena “Sabiedrības izpratne, izglītība un pētniecība” uzdevumiem ir izpildīti. Akadēmisko studiju un pētniecības attīstīšana kiberdrošības, informācijas drošības, IKT drošības jomās ir daļēji izpildīts uzdevums, lai gan jāpiezīmē, ka, kopš tiek īstenota Banku Augstskolas profesionālā maģistra studiju programma “Kiberdrošības pārvaldība”, Vidzemes Augstskolas profesionālā maģistra studiju programma “Kiberdrošības inženierija” un Juridiskajā koledžā plānots izveidot 1. līmeņa studiju programmu “Datu aizsardzība”, atbalsts pētniecības attīstībai kiberdrošības, informācijas drošības, IKT drošības jomās šajā periodā nav bijis pietiekams.

Sabiedrības informēšana par personas datu apstrādes drošību interneta vidē un atbalsts jaunu produktu un tehnoloģiju izstrādei, jaunu IKT drošības risinājumu izveide valsts un / vai nevalstiskajā sektorā ir izpildes procesā, un šo uzdevumu izpildes termiņš ir 2020. gada 4. ceturksnis.

## **Starptautiskā sadarbība**

Rīcības virzienā “Starptautiskā sadarbība” ir iekļauti 9 uzdevumi, un vienam no tiem ir statuss “Informācija dienesta vajadzībām”. Informāciju par 5. rīcības virziena 8 uzdevumu izpildes statusu skatīt 5. shēmā.

*5. shēma*. 5. rīcības virziena uzdevumu izpildes statuss

Astoņi (8) uzdevumi, kas kopumā veido 100% no visiem rīcības uzdevuma “Starptautiskā sadarbība” uzdevumiem, neskaitot uzdevumu ar statusu “Dienesta vajadzībām”, ir izpildīti.

Baltijas valstu saprašanās memorands par sadarbību kiberdrošības jomā tika parakstīts 2015. gada 4. novembrī. Baltijas valstu un ASV sadarbības seminārs par kritisko infrastruktūru un kiberdrošību 2018. gadā tika organizēts Latvijā, un tematiski tas aptvēra jomas, sākot no enerģētikas līdz citiem kritiskās infrastruktūras un kiberdrošības sadarbības aspektiem.

Latvija regulāri piedalās ENISA valdes sēdēs, kurās tiek lemts par aģentūras darba virzieniem un nepieciešamajiem projektiem. Gan AM, gan CERT.LV eksperti regulāri piedalās ENISA organizētajos semināros, konferencēs un citos pasākumos. Kopš 2014. gada CERT.LV kopā ar NBS Kiberaizsardzības vienību un AM ir piedalījušies šādās IT drošības mācībās: “Cyber Coalition” (NATO), “Cyber Europe” (ENISA), “Locked Shields” (CCDCOE). 2018. gada janvārī CCDCOE sadarbībā ar CERT.LV Latvijā organizēja tehniska līmeņa kiberaizsardzības mācības “Crossed Swords”.

## **Kopsavilkums par stratēģijas rīcības virzienu uzdevumu izpildes statusu**

Stratēģijas rīcības plānā kopā ir 68 uzdevumi, no tiem 10 uzdevumiem ir informācijas pieejamības statusa ierobežojums (DIENESTA VAJADZĪBĀM). 42 uzdevumi jeb 72 % no visiem stratēģijas rīcības plāna uzdevumiem, neskaitot uzdevumus ar statusu “Dienesta vajadzībām”, ir izpildīti (skat. 6. shēmu).

*6. shēma*. Stratēģijas rīcības virzienu uzdevumu izpildes statuss

Izpildes procesā atrodas vairāki uzdevumi, kuru izpildes termiņš ir 2020. gada 4. ceturksnis, savukārt kibervides mainības dēļ savu aktualitāti ir zaudējuši 2 stratēģijas rīcības plāna uzdevumi. Ar statusu “Daļēji izpildīts, “Nav izpildīts”, “Nav uzsākts” un “Nav informācijas par izpildes statusu” ir 7 uzdevumi jeb 12 % no visiem stratēģijas rīcības plānā iekļautajiem uzdevumiem, neskaitot uzdevumus ar statusu “Dienesta vajadzībām”.

# **Priekšlikumi kiberdrošības politikas jomā turpmākajiem gadiem**

Stratēģijas grozījumi paredz, ka AM sadarbībā ar visām iesaistītajām ministrijām un NITDP līdz 2019. gada 1. jūnijam jāiesniedz MK informatīvais ziņojums par pamatnostādņu rīcības plāna īstenošanas galīgo novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem.

AM ir sagatavojusi informatīvo ziņojumu “Latvijas kiberdrošības stratēģija 2019.–2022. gadam”, kas ietver ne tikai priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem, bet arī definē konkrētus uzdevumus, izpildes termiņus un atbildīgās, iesaistītās institūcijas un nepieciešamos finanšu līdzekļus to īstenošanai.

Informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” sagatavošanas laikā AM lūdza ISACA, LIA, Latvijas Atvērto tehnoloģiju asociācijai, Latvijas Drošāka interneta centram, Latvijas Drošības un aizsardzības industriju federācijai, LIKTA, LKA, LPS un LTRK sniegt priekšlikumus darāmajiem darbiem kiberdrošības politikā. AM saņēma atbildes no gandrīz visiem uzrunātajiem sadarbības partneriem, kas liecina par to ieinteresētību kiberdrošības jautājumos, kā arī gatavību iesaistīties kiberdrošības politikas veidošanā.

NVO iesniegtie priekšlikumi ietver, piemēram, nepieciešamību ieviest vienotu centralizētu datu pārraides tīklu starp institūcijām, veicināt par IT drošību atbildīgo darbinieku piedalīšanos starptautiskās IT drošības konferencēs un nodrošināt regulāras mācības IT drošības jomā, nodrošināt iespēju sabiedrībai ziņot par pārkāpumiem un problēmsituācijām kibertelpā, piegādes ķēdes drošības jautājumus, nepieciešamību nodrošināt Latvijas industrijas iesaisti starptautiskos projektos un spējas eksportēt stiprināšanu, kā arī daudzus citus.

Izstrādājot informatīvo ziņojumu “Latvijas kiberdrošības stratēģija 2019.–2022. gadam”, AM lūdza ĀM, EM, IeM, IZM, SM, TM un VARAM sniegt viedokli par tobrīd identificētajiem rīcības virzieniem, kā arī informāciju par izvirzāmajiem mērķiem un uzdevumiem mērķu sasniegšanai. Atbildējušās ministrijas piekrita definētajiem rīcības virzieniem, kā arī izteica priekšlikumus, piemēram: izstrādāt koordinētu un organizētu iesaistīto institūciju darbības mehānismu, lai izvairītos no dublēšanās, centralizēt valsts IKT pārvaldību, noteikt, ka valsts institūcijām ir jāpāriet uz IPv6, veicināt kiberdrošības, kā zinātnes, attīstību un citus.

Turpinot darbu pie informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam”, AM vispirms sagatavoja tā sākotnējo projektu un 2018. gada oktobrī, vēl pirms informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projekta iesniegšanas izskatīšanai Valsts sekretāru sanāksmē, lūdza visām ministrijām, VK, Pārresoru koordinācijas centram un valsts drošības iestādēm sniegt redakcionālus labojumus un papildinājumus informatīvā ziņojuma projektam. Lielākā daļa redakcionālo labojumu un papildinājumu tika iekļauta informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projektā, un šajā projektā reprezentēts visu iesaistīto pušu kompromisa redzējums par kibervides turpmāko attīstību.

Informatīvajā ziņojumā “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” ir iekļauti arī tie stratēģijas rīcības plāna uzdevumi, kuru izpildes termiņš ir pēc 2018. gada 4. ceturkšņa. Vienlaikus, ņemot vērā Pārresoru koordinācijas centra ieteikumu, no informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projekta ir svītroti tie uzdevumi, kuri ir definēti arī citos politikas plānošanas dokumentos, piemēram, Informācijas sabiedrības attīstības pamatnostādnēs 2014.–2020. gadam.

Identificējot būtiskas nepilnības stratēģijas grozījumos paredzētajā atskaitīšanās mehānismā, tas ir, galīgo ziņojumu par stratēģijas īstenošanu iesniegt MK pusgadu pēc stratēģijas pārskata perioda beigām, kad jau jābūt izstrādātai un apstiprinātai jaunai kiberdrošības stratēģijai, AM informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projektā ir iekļāvusi citu mehānismu.

Informatīvā ziņojuma “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” projekts paredz, ka AM sadarbībā ar visām iesaistītajām institūcijām un NITDP līdz 2022. gada 1. maijam iesniegs MK informatīvo ziņojumu par stratēģijas uzdevumu īstenošanas novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem. Šāds informatīvā ziņojuma iesniegšanas termiņš dos iespēju uzsākt darbu pie jaunās kiberdrošības stratēģijas izstrādes pēc uzdevumu izpildes statusa un priekšlikumu turpmākajiem gadiem apzināšanas un nodrošinās kiberdrošības politikas pēctecību.

# **Secinājumi**

No stratēģijas rīcības plāna 58 uzdevumiem (neskaitot 10 uzdevumus ar statusu “Dienesta vajadzībām”), kuri ir aplūkoti šī informatīvā ziņojuma 2. pielikumā), 42 uzdevumi jeb 72 % ir izpildīti. Uzdevumu izpilde katrā no pieciem rīcības virzieniem ir dažāda. Rīcības virzienā “Kiberdrošības pārvaldība un resursi” izpildīti ir 64 % uzdevumi, kas ir viszemākais rādītājs no visiem rīcības virzieniem. Rīcības virzienā “Tiesiskums kibertelpā un kibernoziedzības mazināšana” ir izpildīti 75%, savukārt rīcības virzienā “Sagatavotība un rīcībspēja krīzes situācijā” – 73% uzdevumu. Rīcības virzienā “Sabiedrības izpratne, izglītība un pētniecība” statuss “Izpildīts” ir 69% uzdevumu, bet visaugstākais rādītājs un pilnībā (100%) izpildīti uzdevumi ir rīcības virzienā “Starptautiskā sadarbība”.

Informatīvajā ziņojumā par pamatnostādņu rīcības plānā noteikto uzdevumu ieviešanas gaitu, kas tika izskatīts MK 2016. gada 29. marta sēdē, tika uzsvērts, ka pilnvērtīgi sasniegt stratēģijā nospraustos mērķus kavē trīs problēmas: a) kiberdrošības jautājumi nav prioritāte, b) finansējuma trūkums, c) personāla trūkums.

Aplūkojot rīcības plāna izpildes statusu, īpašu uzmanību pievēršot daļēji izpildītajiem, neizpildītajiem un neuzsāktajiem uzdevumiem, var secināt, ka galvenā problēma ir nepiešķirtie, papildu nepieciešamie budžeta līdzekļi. Lai arī daudzus rīcības plāna uzdevumus bija paredzēts veikt no likumā par valsts budžetu kārtējam gadam institūcijām paredzētajiem finanšu līdzekļiem, tomēr daļai uzdevumu bija nepieciešams ES struktūrfondu finansējums vai papildu budžeta līdzekļi.

Raugoties uz otru, jau identificēto problēmu, ka kiberdrošības jautājumi nav prioritāte, atkārtoti jāuzsver – lai gan Latvijā ir izveidots daļēji centralizēts kiberdrošības politikas koordinācijas modelis, kur Aizsardzības ministrijai ir vadošā loma, kiberdrošības elements ir atrodams gandrīz katras nozares ministrijas atbildības jomā. Tā rezultātā kiberdrošības politika pēc savas būtības ir horizontāla un nozaru ministriju sadarbība, kā arī veicamo uzdevumu apzināšana un atbildības uzņemšanās par to izpildi savā nozarē ir vienīgais veids, kā kopumā stiprināt kiberdrošību valstī.

Personāla trūkums, kas tika identificēts kā problēma jau iepriekš, ir aplūkots arī informatīvajā ziņojumā “Latvijas kiberdrošības stratēģija 2019.–2022. gadam”. Publiskajā sektorā ir izteikta vajadzība pēc kvalificētiem speciālistiem, taču konkurencē ar privāto sektoru par pieejamajiem, darba tirgū esošajiem speciālistiem publiskais sektors parasti zaudē. Pieņemot, ka vajadzība pēc kvalificētiem speciālistiem nākotnē neizzudīs, ir nepieciešami risinājumi, kā ne tikai piesaistīt, bet arī noturēt valsts sektorā strādājošos.

Nākamajā periodā (no 2019. līdz 2022. gadam) institūcijām ir atbildīgi jāīsteno informatīvajā ziņojumā “Latvijas kiberdrošības stratēģija 2019.–2022. gadam” noteiktie uzdevumi piecos rīcības virzienos:

1) kiberdrošības veicināšana, digitālās drošības risku mazināšana,

2) IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana,

3) sabiedrības izpratne, izglītība un pētniecība,

4) starptautiskā sadarbība,

5) tiesiskums kibertelpā un kibernoziedzības mazināšana.

Vienlaikus jāakcentē, ka iepriekšminētajā laika periodā atbildīgās un iesaistītās institūcijas turpinās realizēt iepriekšējā periodā iniciētos pastāvīgos uzdevumus, kā arī definētie uzdevumi neierobežo institūcijas veikt citas neminētas darbības.

Ministru prezidenta biedrs,

aizsardzības ministrs A. Pabriks