*Projekts*

Ministru kabineta

2018.gada \_\_\_\_\_\_\_\_\_\_

rīkojums Nr.\_\_\_\_\_

**Pamatnostādnes**

**“Latvijas kiberdrošības stratēģija**

**2019.-2022.gadam”**

Rīga, 2018

**Saturs**

[Kopsavilkums 3](#_Toc530645130)

[Saīsinājumi 4](#_Toc530645131)

[Ievads 5](#_Toc530645132)

[1. Vīzija, mērķi, prioritātes un principi 6](#_Toc530645133)

[2. Pārvaldības sistēma, funkcijas un pienākumi kiberdrošības pārvaldībā 6](#_Toc530645134)

[3. Kiberdrošības situācijas analīze 9](#_Toc530645135)

[3.1. Situācijas raksturojums 9](#_Toc530645136)

[3.2. Izaicinājumi 10](#_Toc530645137)

[4. Nacionālās kiberdrošības politikas rīcības virzieni 11](#_Toc530645138)

[4.1. Kiberdrošības veicināšana, digitālās drošības risku mazināšana 12](#_Toc530645139)

[4.2. IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana 13](#_Toc530645140)

[4.3. Sabiedrības izpratne, izglītība un pētniecība 13](#_Toc530645141)

[4.4. Starptautiskā sadarbība 14](#_Toc530645142)

[4.5. Tiesiskums kibertelpā un kibernoziedzības mazināšana 15](#_Toc530645143)

[5. Turpmākā rīcība 15](#_Toc530645144)

[6. Ietekmes novērtējums uz valsts budžetu un pašvaldību budžetu 15](#_Toc530645145)

[7. Pārskatu iesniegšanas kārtība 17](#_Toc530645146)

[8. Noslēguma jautājumi 17](#_Toc530645147)

Pielikumi:

1. Rīcības plāns pamatnostādņu īstenošanai
2. Rīcības plāns pamatnostādņu īstenošanai (informācija dienesta vajadzībām)

# Kopsavilkums

Pamatnostādnes “Latvijas kiberdrošības stratēģija 2019.-2022.gadam” (Pamatnostādnes) raksturo Latvijas kiberdrošības situāciju, identificē nākotnes izaicinājumus un definē nacionālās kiberdrošības politikas rīcības virzienus laika periodam līdz 2022. gadam. Kiberdrošība ir visaptverošas valsts aizsardzības sistēmas elements. Visaptverošajā valsts aizsardzībā, kur katrs sabiedrības loceklis tiek organizēts, lai aizsargātu valsti pret visa veida uzbrukumiem, gan militāriem, gan nemilitāriem, kiberaizsardzībai ir aizvien lielāka nozīme, ņemot vērā sekas, kādas valstij un sabiedrībai var nodarīt pret to vērsts kiberuzbrukums.

Kiberdrošības politikas vīzija ir droša, atvērta, brīva un uzticama kiber­telpa, kurā ir garantēta valstij un sabiedrībai būtisku pakal­pojumu droša, uzticama un nepārtraukta saņemšana un sniegšana, un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē.

Kiberdrošības politikas mērķis laika periodam no 2019.gada līdz 2022.gadam ir stiprināt un attīstīt kiberaizsar­dzības spējas, paaugstinot noturību pret kiberuzbrukumiem un veicinot sabiedrības izpratni par draudiem kibertelpā. Īstenojot kiberdrošības politiku, laika periodam no 2019.gada līdz 2022.gadam tiek definētas šādas prioritātes: aizsardzība, atturēšana un attīstība.

Ņemot vērā Eiropas Savienības izvirzītās prioritātes un nacionālajos politikas plānošanas un citos dokumentos noteiktos mērķus, pamatnostādnes izvirza piecus rīcības virzienus periodam līdz 2022. gadam:

* kiberdrošības veicināšana, digitālās drošības risku mazināšana,
* informācijas un komunikāciju tehnoloģiju izturētspēja, sabiedrībai kritiski svarīgu informācijas un komunikāciju tehnoloģiju un pakalpojumu nodrošināšanas stiprināšana,
* sabiedrības izpratne, izglītība un pētniecība,
* starptautiskā sadarbība,
* tiesiskums kibertelpā un kibernoziedzības mazināšana.

Visi iepriekšminētie rīcības virzieni ir detalizēti aprakstīti pamatnostādņu sadaļās un apakšsadaļās, savukārt uzdevumi un pasākumi, izpildes termiņi, atbildīgās un iesaistītās institūcijas, nepieciešamie finanšu līdzekļi un sasniedzamais rezultāts ir iekļauti pamatnostādņu 1. pielikumā un 2.pielikumā (informācija dienesta vajadzībām).

Pamatnostādņu paredzēto pasākumu īstenošana tiks nodrošināta pamatnostādnēs minētajām institūcijām piešķirto valsts budžeta un pašvaldību budžeta līdzekļu ietvaros. Jautājums par papildu valsts budžeta līdzekļu piešķiršanu pamatnostādnēs minētajām institūcijām izskatāms Ministru kabinetā gadskārtējā valsts budžeta likumprojekta sagatavošanas un izskatīšanas procesā.

# Saīsinājumi

AIM Aizsardzības ministrija

ANO Apvienoto Nāciju Organizācija

ĀM Ārlietu ministrija

CERT.LV Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CSP Centrālā statistikas pārvalde

DVI Datu valsts inspekcija

EDSO Eiropas Drošības un sadarbības organizācija

EM Ekonomikas ministrija

ENISA Eiropas Tīklu un informācijas drošības aģentūra

ES Eiropas Savienība

ESAO Ekonomiskās sadarbības un attīstības organizācija

FKTK Finanšu un kapitāla tirgus komisija

IEM Iekšlietu ministrija

IKT Informācijas un komunikācijas tehnoloģijas

IP Interneta protokols

IT Informācijas tehnoloģijas

IZM Izglītības un zinātnes ministrija

KAV Nacionālo bruņoto spēku Kiberaizsardzības vienība

KDAP Kopējā drošības un aizsardzības politika

KI Kritiskā infrastruktūra

LB Latvijas Banka

LFNA Latvijas Finanšu nozares asociācija

LI Lietu internets

LIA Latvijas interneta asociācija

LIAA Latvijas investīciju un attīstības aģentūra

LIKTA Latvijas Informācijas un komunikācijas tehnoloģijas asociācija

LM Labklājības ministrija

LPS Latvijas Pašvaldību savienība

LVRTC Latvijas Valsts radio un televīzijas centrs

MIDD Militārās izlūkošanas un drošības dienests

MilCERTMilitāro informācijas tehnoloģiju drošības incidentu novēršanas komanda

NATO Ziemeļatlantijas līguma organizācija

NBS Nacionālie bruņotie spēki

NetSafe Latvijas Drošāka interneta centrs Net-Safe Latvia

NITDP Nacionālā informācijas tehnoloģiju drošības padome

SAB Satversmes aizsardzības birojs

SM Satiksmes ministrija

SPRK Sabiedrisko pakalpojumu regulēšanas komisija

TM Tieslietu ministrija

VARAM Vides aizsardzības un reģionālās attīstības ministrija

VDD Valsts drošības dienests

VIS Valsts informācijas sistēmas

VK Valsts kanceleja

VP Valsts policija

VRS Valsts robežsardze

VRAA Valsts reģionālās attīstības aģentūra

VSAA Valsts sociālās apdrošināšanas aģentūra

# Ievads

Pamatnostādnes raksturo Latvijas kiberdrošības[[1]](#footnote-2) situāciju, identificē nākotnes izaicinājumus un definē nacionālās kiberdrošības politikas rīcības virzienus laika periodam līdz 2022. gadam, tādējādi turpinot pamatnostādņu “Latvijas kiberdrošības stratēģija 2014-2018” noteiktos virzienus kiberdrošības stiprināšanā.

Kiberdrošība ir visaptverošas valsts aizsardzības sistēmas elements. Visaptverošajā valsts aizsardzībā, kur katrs sabiedrības loceklis tiek organizēts, lai aizsargātu valsti pret visa veida uzbrukumiem, gan militāriem, gan nemilitāriem, kiberaizsardzībai ir aizvien lielāka nozīme, ņemot vērā sekas, kādas valstij un sabiedrībai var nodarīt pret to vērsts kiberuzbrukums.

Informācijas un komunikācijas tehnoloģiju (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 ikdienā.

Ir pamats runāt par digitālas sabiedrības veidošanos Latvijā un ārvalstīs, mainoties līdzšinējai kārtībai, kādā sabiedrība, uzņēmēji un valsts pārvalde ikdienā funkcionē un savstarpēji mijiedarbojas. Taču digitālas sabiedrības plašās iespējas veicina arī riskus, kas saistīti ar kiberuzbrukumiem pret IKT un to lietotājiem privātajā un nevalstiskajā sektorā, kā arī valsts pārvaldes iestādēs. Veiksmīgas digitālas sabiedrības priekšnosacījums ir sabiedrības, uzņēmēju un valsts pārvaldes uzticēšanās IKT risinājumu un digitālo tehnoloģiju spējai garantēt pakalpojumu pieejamību, kā arī saglabātās, apstrādātās vai pārsūtītās informācijas drošību.

Pamatnostādnes izstrādātas ņemot vērā pasākumus, kas ietverti Latvijas ilgtspējīgas attīstības stratēģijā, Nacionālajā drošības koncepcijā, Valsts aizsardzības koncepcijā, Eiropas Savienības (ES) un Ziemeļatlantijas līguma organizācijas (NATO) dokumentos kiberdrošības jomā un starptautisko organizāciju vadlīnijās.

# Vīzija, mērķi, prioritātes un principi

Mūsdienu valsts un sabiedrības funkcionēšana ir kritiski atkarīga no IKT. Tomēr tās nav absolūti drošas un var tikt pakļautas uzbrukumiem. Uzbrukuma draudus IKT nevar pilnībā novērst, bet uzbrukuma risku var ievērojami mazināt, lai netraucētu sabiedrības attīstību, netiktu nodarīti zaudējumi ekonomikai un gūt labumu no IKT gan valsts pārvaldē, gan privātajā sektorā.

Kiberdrošības politikas vīzija ir droša, atvērta, brīva un uzticama kiber­telpa, kurā ir garantēta valstij un sabiedrībai būtisku pakal­pojumu droša, uzticama un nepārtraukta saņemšana un sniegšana, un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē.

Kiberdrošības politikas mērķis laika periodam no 2019.gada līdz 2022.gadam ir stiprināt un attīstīt kiberaizsar­dzības spējas, paaugstinot noturību pret kiberuzbrukumiem un veicinot sabiedrības izpratni par draudiem kibertelpā.

Apakšmērķi kiberdrošības politikas mērķa sasniegšanai ir:

* kiberdrošības risku mazināšana;
* nacionālo kiberaizsardzības spēju attīstīšana;
* IKT infrastruktūras, informācijas sistēmu un pakalpojumu drošības nodrošināšana;
* sabiedrības izpratnes veicināšana par kiberriskiem;
* cīņa pret kibernoziegumiem.

Īstenojot kiberdrošības politiku, laika periodam no 2019.gada līdz 2022.gadam tiek definētas šādas prioritātes: aizsardzība, atturēšana un attīstība.

Aizsardzība – attīstīt un pilnveidot spējas, kas ietver gan nepieciešamos resursus, gan izpratni, gan zināšanas, lai aizstāvētos pret pieaugošajiem kiberdraudiem un, lai efektīvi reaģētu uz IKT drošības incidentiem un nodrošinātu IKT aizsardzību un spēju funkcionēt. Sabiedrībai, privātajam un publiskajam sektoram ir jāattīsta zināšanas un spējas sevi aizstāvēt.

Atturēšana – atklāt, izmeklēt un pārtraukt ļaunprātīgas darbības kibertelpā, veicot likumpārkāpēju identificēšanu un saukšanu pie atbildības, tādējādi atturot citus no šādu darbību veikšanas.

Attīstība – pastāvīgi un sistemātiski attīstīt un pilnveidot dažādu nozaru IKT lietotāju prasmes un veicināt specializāciju IKT drošības jautājumos.

Kiberdrošības politikas īstenošanā tiek ievēroti šādi principi:

* kiberdrošība nav pašmērķis, bet gan neatņemama nacionālās drošības sastāvdaļa – mūsdienu valsts, sabiedrības un ekonomikas funkcio­nē­šanas pamats;
* kiberdrošības veicināšana starptautiski, sadarbojoties ar sabiedro­tajiem un partne­riem, ir nepieciešama nacionālo kiberdrošības mērķu sasniegšanai;
* kiberdrošības jautājumus koordinācijā iesaistām pilsonisko sa­bied­rību, privātās, publiskās un akadēmiskās jomas pārstāvjus;
* kiberdrošība tiek nodrošināta, ievērojot arī cilvēktiesības;
* kiberuzbrukumu laicīga paredzēšana un novēršana ir svarīga.

# Pārvaldības sistēma, funkcijas un pienākumi kiberdrošības pārvaldībā

Kiberdrošības jomā Latvijā tiek īstenots daļēji centralizēts pārvaldības modelis, kurā vadošās iestādes veic kiberdrošības pamatnostādņu plānošanu un koordinē un īsteno tajā paredzētos pasākumus, katrai iestādei savas kompetences jautājumos nodrošinot paredzēto pasākumu praktisku ieviešanu un izpildi. Nacionālās kiberdrošības pārvaldības pamatā ir savstarpējā sadarbība, kur katrai valsts iestādei pildot savas funkcijas, tajā skaitā kibertelpā, tiek īstenota tieša sadarbība ar citām iestādēm vai sadarbība Nacionālās informācijas tehnoloģiju drošības padomē (NITDP). NITDP ir izveidota, pamatojoties uz Informācijas tehnoloģiju drošības likumu, kas nosaka kiberdrošības politikas veidošanu nacionālajā līmenī un uzdod NITDP koordinēt kiberdrošības politikas izstrādi, uzdevumu un pasākumu plānošanu un veikšanu. NITDP ir centrālā nacionālā institūcija valsts un privātā sektora informācijas apmaiņai un sadarbībai kiberdrošības jomā, un tās darbību un sekretariātu nodrošina Aizsardzības ministrija.

1.shēma

**Kiberdrošības pārvaldība**

MINISTRU KABINETS

NACIONĀLĀ IT DROŠĪBAS PADOME

Nacionālās IT drošības padomes institūcijas u.c. iesaistītie dalībnieki, atbilstoši funkcijām un pienākumiem

NVO

Valsts informācijas sistēmas

E-pakalpojumi

Elektronisko sakaru komersanti

Komersanti

Valsts IKT infrastruktūra

Kritiskā infrastruktūra

VALSTS SEKTORS

PRIVĀTAIS SEKTORS

Sabiedrība / lietotāji

Kiberdrošības pārvaldības sistēmā iesaistīto valsts pārvaldes institūciju un citu iesaistīto dalībnieku funkcijas un pienākumi ir:

* Aizsardzības ministrija (AIM) koordinē informācijas tehnoloģiju drošības un aizsardzības politikas veido­šanu un īstenošanu, kā arī līdzdarbojas starptautiskās sadarbības nodrošināšanā. AM Krīzes vadības departamenta Nacionālās kiberdrošī­bas politikas koordinācijas nodaļa nodrošina nacionālās kiberdrošības politikas veidošanu un sniedz atbalstu kiberdrošības politikas īstenošanai.
* Ārlietu ministrija (ĀM) koordinē starptautisko sa­darbību un Latvijas dalību dažādās ar kiberdrošību saistītās starptautiskās iniciatīvās.
* Finanšu un kapitāla tirgus komisija (FKTK) regulē un pārrauga finanšu un kapitāla tirgus dalībnieku darbību kibertelpā, Latvijas Banka (LB) veicina mak­sājumu sistēmu drošu un nepārtrauktu darbību, un kredītiestā­des atbild par savas nozares elektronisko pakalpojumu drošību un pieejamību.
* 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.
* Valsts drošības dienests (VDD) īsteno valsts (un sabiedrības) iekšējās drošības uzraudzību.
* Informācijas tehnoloģiju drošības incidentu no­vēršanas institūcija CERT.LV novēro un analizē kibertelpā notiekošo, reaģē uz incidentiem un koor­dinē to novēršanu, veic pētniecisko darbu, organizē izglītojošus pasākumus un apmācības, kā arī uzrauga Informācijas tehnoloģiju drošības likumā noteikto pienākumu izpildi. CERT.LV sniedz atbalstu Latvijas un ārvalstu, valsts un pašvaldību institūcijām, komer­santiem un fiziskām personām.
* Izglītības un zinātnes ministrija (IZM) veicina sa­biedrības zināšanas un izpratni par kibertelpu zināšanu bāzes veidošanos zinātnes, tehnoloģiju, inženierijas un matemātikas jomās visos izglītības līmeņos, kā arī stiprina augstskolu pētniecības kapacitāti, nodrošinot valsts budžeta un ES fondu finansējumu pētniecības infrastruktūras, tajā skaitā nepieciešamā cilvēkkapitāla, attīstībai un stiprināšanai.
* 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. Valsts sociālās apdrošināšanas aģentūra (VSAA) nodrošina dažādu valsts noteikto pabalstu, pensiju un atlīdzību izmaksu iedzīvotājiem.
* Latvijas Drošāka interneta centra Net-Safe Latvia darbību nodrošina Latvijas Interneta asociācija (ar Aizsardzības ministrijas atbalstu), izglīto sabiedrību par iespējamajiem riskiem un draudiem interneta vidē, veicina drošu interneta lietošanu un drošu interneta saturu.
* Militāro informācijas tehnoloģiju drošības incidentu novēršanas komanda (MilCERT) nodrošina Aizsardzības ministrijas un tās padotības iestāžu, tostarp Nacionālo bruņoto spēku (NBS) informācijas un komunikācijas tehnoloģiju 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.
* Nacionālie bruņotie spēki (NBS) un Kiberaizsardzī­bas vienība (KAV) sniedz atbalstu nacionālās krīzes situācijās.
* 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 IT kri­tisko infrastruktūru.
* Tieslietu ministrija (TM) un Datu valsts inspekcija (DVI) izstrādā, organizē un koordinē tiesību politiku personas datu aizsardzības, informācijas atklātības un elektronisko dokumentu uzraudzības jomā.
* Valsts akciju sabiedrība „Latvijas Valsts radio un televīzijas centrs” (LVRTC) ir uzticamu sertifikācijas pakalpojumu sniedzējs, kurš nodrošina elektroniskās identifikācijas līdzekļu un autentifikācijas rīku darbībai nepieciešamo infrastruktūru.
* Vides aizsardzības un reģionālās attīstības ministrija (VARAM) organizē valsts IKT pārvaldību un koordinē publisko pakalpojumu elektronizāciju, savukārt Valsts re­ģionālās attīstības aģentūra (VRAA) nodrošina valsts IKT koplietošanas risinājumu darbību un attīstību.

# Kiberdrošības situācijas analīze

## Situācijas raksturojums

Lai mazinātu kibertelpā esošo draudu iespējas ietekmēt informācijas sistēmu darbību, kiberuzbrukumu izplatību un sekas, Latvijai ir nepieciešams turpināt noteikt vienotus kiberdrošības politikas prioritāros rīcības virzienus, uzdevumus un mērķus vidēja termiņa plānošanas periodam, apvienojot nozaru ministriju un struktūru pasākumus nacionālās kiberdrošības stiprināšanai. Stratēģiska pieeja Latvijas kiberdrošības stiprināšanai ir svarīga arī starptautisko apsvērumu dēļ. Nepieciešams ņemt vērā ES Digitālā vienotā tirgus stratēģijas Eiropai mērķi līdz 2020. gadam nodrošināt ES iedzīvotāju pilnvērtīgu iespēju izmantot digitālā tirgus sniegto potenciālu ar vienlīdzīgiem, drošiem un uzticamiem risinājumiem, ES Tīklu un informācijas drošības direktīvas mērķi izlīdzināt un stiprināt ES dalībvalstu kiberdrošības spējas un ņemot vērā Latvijas ģeogrāfisko atrašanās vietu un saistības attiecībā pret NATO valstīm.

Pēc Eiropas policijas biroja Eiropas kibernoziedzības apkarošanas centra aprēķiniem, IKT risinājumu un digitālo tehnoloģiju izmantošanas rezultātā kibernoziedzība aug straujāk nekā jebkad agrāk, gadā sasniedzot vismaz 265 miljardus euro nodarītajos zaudējumos ES dalībvalstīs un apmēram 900 miljardus euro pasaulē kopumā. Eiropas Savienības Tīklu un informācijas drošības aģentūras (ENISA) 2016. gada pētījumā “Kritiskās informācijas infrastruktūras incidentu izmaksas” secināts, ka lielākos zaudējumus no kiberuzbrukumiem cieš finanšu, IKT un enerģētikas sektora uzņēmumi, savukārt CISCO 2018. gada ikgadējā drošības pārskatā “Kiberdrošības ziņojums: ietekme uz publisko sektoru” konstatēta būtiska globāla tendence kiberuzbrukumu pieaugumam valsts pārvaldes iestādēm, izmantojot pikšķerēšanas (*phishing*), izspiedējvīrusu (*ransomware*) un ļaunatūras (*malware*) augšuplādes uzbrukumu metodes, datu izgūšanas vai integritātes kompromitēšanai.

Iejaukšanās citu valstu vēlēšanu kampaņās, izmantojot dažādus līdzekļus sociālos tīklus, daudzviet ir kļuvis par nacionālās drošības jautājumu. Latvijā līdz šim brīdim var atzīmēt divus ar 13.Saeimas vēlēšanām saistītus kiberuzbrukumus – kiberuzbrukums vietnei Delfi.lv pirms populārāko partiju premjeru kandidātu debatēm un kiberuzbrukums vietnei Draugiem.lv vēlēšanu dienā.

Latvijas kibertelpa turpina saskarties ar plaša rakstura draudiem – pikšķerēšanas, izspiedējvīrusu un ļaunatūru izplatības kampaņām, sistēmu, tīklu un mājaslapu uzlaušanas mēģinājumiem, piekļuves lieguma uzbrukumiem kritiski svarīgām informācijas sistēmām un krāpniecisko e-pastu un sociālās inženierijas kampaņām ar mērķi izgūt personu vai autentifikācijas datus konkrētas personas, uzņēmuma vai iestādes diskreditēšanai vai noziegumu veikšanai. Lai arī Latvijā ir izveidota stabila un pārskatāma kiberdrošības struktūra, kuras pamatā ir līdzšinējās pamatnostādnes “Latvijas kiberdrošības stratēģija 2014.–2018”, Informācijas tehnoloģiju drošības likuma regulējums un Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (CERT.LV un MilCERT) darbība, nacionālā IT drošība ir nemitīgi jāpilnveido, lai veicinātu spējas paredzēt un atvairīt kiberuzbrukumus ar neparedzētiem uzbrukuma raksturlielumiem, kā arī, lai uzlabotu spējas novērst kiberuzbrukumu sekas.

IKT risinājumiem un digitālajām tehnoloģijām ir būtiska loma Latvijas sabiedrības, tautsaimniecības un valsts pārvaldes darbībā. Saskaņā ar Latvijas Centrālās statistikas pārvaldes datiem, 2017. gadā Latvijā apmēram 84% iedzīvotāju tika nodrošināta piekļuve internetam un 78,5% iedzīvotāju vecumā no 16 – 74 gadiem regulāri (vismaz reizi nedēļā) lietoja internetu. Saskaņā ar Digitālās ekonomikas un sabiedrības indeksu 2018, 75,3% iedzīvotāju lieto internetbanku pakalpojumus regulāri (pēdējos sešos mēnešos vismaz sešas reizes ir autorizējušies internetbankā) un 99% no banku pārskaitījumiem Latvijā tiek veikti elektroniski. 70,2% interneta lietotāju izmantoja mobilās ierīces, lai piekļūtu internetam ārpus mājas vai darba. Preču vai pakalpojumu pirkšanu tiešsaistē veikuši 55% iedzīvotāju un pakāpeniski pieaug mazo un vidējo uzņēmēju skaits, kas produktus pārdod tiešsaistē, kā arī pieaug e-komercijas apgrozījums. 77% iedzīvotāju dokumentus valsts pārvaldes iestādēm iesniedz elektroniski, un uzņēmējiem ir pieejams plašs publisko elektronisko pakalpojumu klāsts. Notiek plaša valsts nodrošināto pakalpojumu un valsts pārvaldes procesu elektronizācija, ieviešot, piemēram, valsts veselības aprūpes informācijas sistēmu “E-veselība” un oficiālo e-adresi, kuras izmantošana no 2018. gada 1. jūnija ir obligāta valsts iestādēm.

Minētie rādītāji liecina par digitālas sabiedrības veidošanos Latvijā, kur IKT risinājumu un digitālo tehnoloģiju lietošana kalpo par pamatu labklājības, saimnieciskās darbības un ekonomikas izaugsmei. Lai arī digitalizācija atvieglo sabiedrības savienojamību un pieeju precēm un pakalpojumiem, tā paver iespējas uzbrukumiem IKT risinājumu un digitālo tehnoloģiju sistēmām. Latvijas kibertelpā tiek novērots plašs kiberuzbrukumu spektrs, un, ņemot vērā izmaiņas ģeopolitiskajā situācijā pasaulē kopš 2014. gada, pastiprināta darbība tiek novērota pret valsts pārvaldes IT un informācijas sistēmām. IT drošības incidentu novēršanas institūcija (CERT.LV) kopš 2017. gada ir novērojusi pieaugumu šifrējošo izspiedējvīrusu pielietošanā uzbrukumos valsts pārvaldes vai valstij kritiski svarīgām informācijas sistēmām, kas īpašu uzmanību pasaulē ieguva WannaCry un NotPetya kiberuzbrukumu kampaņu laikā 2017. gada maijā un jūnijā. Šeit gan jāatzīmē, ka cietošo skaits Latvijā bija neliels un neviens no tiem nebija no valsts sektora vai kritiskās infrastruktūras.

Kibertelpā tiek novēroti regulāri informācijas sistēmu un mājaslapu uzlaušanas mēģinājumi, krāpniecisko e-pastu kampaņas ar mērķi izkrāpt personu datus, autentifikācijas datus vai inficēt informācijas sistēmu ar ļaunatūru. Ļoti bieži datu noplūdes un sistēmu uzlaušanas iemesli ir nepietiekami droši konfigurētas lietotāju informācijas sistēmas un nepietiekamas zināšanas par drošu IKT risinājumu un digitālo tehnoloģiju lietošanu. 2018. gada 2. ceturksnī kopumā tika konstatēts 182 436 apdraudētas IP adreses, no kurām 135 796 tika konstatētas konfigurācijas nepilnības, kuras kiberuzbrucēji varētu izmantot uzbrukumu veikšanai. Plaši novērojama arī ļaundabīgā koda izplatība informācijas sistēmās un ielaušanās mēģinājumi informācijas sistēmās, izmantojot ievainojamības lietotāju informācijas sistēmās un pakļaujot tos robotu tīkliem tālāku ļaunprātīgu darbību veikšanai.

## Izaicinājumi

Digitālā vide turpina radīt jaunas plaša mēroga un plaši integrētas uzņēmējdarbības un sociālās tīklošanās iespējas, kas padara to par pievilcīgu mērķi kibernoziegumiem un ārvalstu atbalstītai spiegošanai vai sabotāžai. 2018. gada 4. oktobrī Nīderlandes valdības paziņojums par 2018. gada aprīlī novērsto kiberuzbrukumu Ķīmisko ieroču aizlieguma organizācijai tikai apstiprina, kas valstu atbalstīti kiberuzbrukumi var skart ikvienu, neatkarīgi no nodarbošanās vai atrašanās vietas. Ņemot vērā iepriekš minēto, kiberaizsardzība ir būtisks visaptverošas valsts aizsardzības sistēmas elements, kurā gan valsts pārvaldes institūcijām, gan pašvaldībām, gan privātajam sektoram, kā arī katram indivīdam atsevišķi ir sava nozīmīga loma kopēja mērķa sasniegšanā.

Kibernoziegumu skaits un intensitāte nākotnē pieaugs līdz ar digitālās vides attīstību. Kibernoziegumus var iedalīt divos veidos - noziegumi, kur IKT ierīces ir gan nozieguma izdarīšanas līdzeklis, gan mērķis, un noziegumi, kuru nodarījumu var palielināt, izmantojot IKT ierīces. Ņemot vērā teroristisko grupējumu izmantoto līdzekļu spektra paplašināšanos, var pieņemt, ka tie savu mērķu sasniegšanai arvien biežāk izmantos kibertelpu un tai pieslēgtos resursus.

Kā viens no nākotnes izaicinājumiem ir jāmin arī lietu internets[[2]](#footnote-3) (LI), jo, turpinot attīstīties arvien jaudīgākām datu pārraides tehnoloģijām, kuras var integrēt saimniecībās plaši izmantotas preces, ir vērojams LI popularitātes pieaugums, kā rezultātā LI pieslēgto sensoru un ierīču drošība kļūst par vienu no izaicinājumiem. Var prognozēt, ka īstermiņā internetam pieslēgtas ērti vadāmās ierīces būs visu mājsaimniecību un saimnieciskās darbības veicēju neatņemama daļa, tādējādi radot lielapjoma datus (*Big Data*), kas tiek uzkrāti no un mijiedarbojoties LI ierīcēm.

Interneta ēnu sektors (*Dark Net*), kura pamatideja ir anonimitāte, arī nākotnē tiks izmantots nelegālu darbību veikšanai, tai skaitā, jau izstrādātas ļaunatūras un citu uzbrukuma veidu izplatīšanai. Tas var vecināt hakeru aktivitātes pieaugumu.

Mākoņdatošana un tās piedāvātie risinājumi, kuri strauju attīstību uzsāka pirms vairākiem gadiem, neapšaubāmi, turpinās attīstību, un šie risinājumi kļūs arvien populārāki. Līdztekus mākoņdatošanas tehnoloģisko iespēju attīstībai ir jāturpinās arī mākoņdatošanas drošības politikai, kas attiecībā uz mākoņdatošanu vienmēr ir bijis sensitīvākais jautājums.

Attīstoties Latvijas ekonomikai, arvien vairāk ir izjūtams jomu speciālistu trūkums, sevišķi IKT speciālistu trūkums, kas gan nav tikai Latvijas fenomens, bet izteikta situācija arī citur pasaulē. Kvalificētu darbinieku trūkums noved pie nesamērīgi augstas uzņēmēju savstarpējās konkurences IKT speciālistu piesaistīšanā un, salīdzinot ar publisko sektoru, neproporcionāli augstu piedāvāto darba samaksu IKT jomā strādājošajiem. IKT speciālistu trūkums padara publiskā sektora iestādes nekonkurētspējīgas cīņā par nepieciešamajiem speciālistiem un attiecīgi vājina publiskā sektora IKT resursu uzturēšanas un pilnveidošanas iespējas.

Ņemot vērā apdraudējumu, kas nāk ar IKT plašāku izmantošanu, pastāv nepieciešamība aizvien vairāk ierobežot iespējamos draudus. Nepieciešams atrast līdzsvaru starp efektīvu pārvaldību un tiesībām uz privātumu kibertelpā, lai neierobežotu inovācijas, attīstību un efektivizāciju.

# Nacionālās kiberdrošības politikas rīcības virzieni

Definējot nacionālās kiberdrošības politikas rīcības virzienus līdz 2022. gadam, jāņem vērā nacionālie politikas plānošanas un citi dokumenti, kuri kiberdrošības politikas jomā izvirza ilgtermiņa mērķus. Šī sasaiste ir būtiska, lai nodrošinātu konsekventu kiberdrošības politikas attīstību.

Nacionālie dokumenti, kuri definē ilgtermiņa mērķus kiberdrošības jomā:

* Latvijas ilgtspējīgas attīstības stratēģija – Latvija 2030;
* Nacionālā drošības koncepcija;
* Valsts aizsardzības koncepcija;
* Informācijas sabiedrības attīstības pamatnostādnes 2014.-2020. gadam;
* Elektronisko sakaru nozares politikas plāns 2018.-2020. gadam;
* Nacionālo bruņoto spēku Kiberaizsardzības vienības koncepcija, 2013.gads;
* Informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanu Latvijā", 2018.gads.

ES 2013. gadā apstiprinātajā “Eiropas Savienības kiberdrošības stratēģijā” ir izvirzījusi piecas prioritātes:

* Kibernoturības panākšana;
* Kibernoziedzības būtiska samazināšana;
* Kiberaizsardzības politikas izstrāde un spēju veidošana saistībā ar kopējo drošības un aizsardzības politiku (KDAP);
* Rūpniecisko un tehnoloģisko resursu veidošana kiberdrošības vajadzībām;
* Saskaņotas starptautiskas kibertelpas politikas izveide Eiropas Savienībā un ES pamatvērtību popularizēšana.

Ņemot vērā ES izvirzītās prioritātes un nacionālajos politikas plānošanas un citos dokumentos noteiktos mērķus, pamatnostādnes izvirza piecus rīcības virzienus periodam līdz 2022. gadam:

* kiberdrošības veicināšana, digitālās drošības risku mazināšana,
* IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana,
* sabiedrības izpratne, izglītība un pētniecība,
* starptautiskā sadarbība,
* tiesiskums kibertelpā un kibernoziedzības mazināšana.

Visi iepriekšminētie rīcības virzieni ir detalizēti aprakstīti šīs nodaļas apakšsadaļās, savukārt uzdevumi, izpildes termiņi, atbildīgās un iesaistītās institūcijas, nepieciešamie finanšu līdzekļi un sasniedzamais rezultāts ir iekļauti pamatnostādņu 1. pielikumā un 2.pielikumā (informācija dienesta vajadzībām).

Vienlaikus ES Tīklu un informācijas sistēmu drošības direktīvas (ES 2016/1148) (Direktīva) 7. pants izvirza septiņus jautājumus, kuriem dalībvalstīm ir jāpievēršas valsts tīklu un informācijas sistēmu drošības stratēģijā. Latvija, izstrādājot pamatnostādnes laika periodam līdz 2022. gadam ir iekļāvusi direktīvas izvirzītos jautājumus pamatnostādņu sadaļās un pielikumos, tādējādi izpildot direktīvas prasības.

## Kiberdrošības veicināšana, digitālās drošības risku mazināšana

Valsts mērķis ir visaptverošas valsts aizsardzības sistēmas izveide, kurā notiek cieša sadarbība starp valsts, privāto sektoru un sabiedrību kopumā kibertelpas drošības un aizsardzības stiprināšanā, tai skaitā nodrošinot IT kritiskās infrastruktūras aizsardzību. Lai veicinātu kiberdrošības noturību Latvijā, valsts pārvaldes iestādēm un privātajam sektoram ir jāveido spējas un efektīvi jāsadarbojas, lai nodrošinātu, ka valsts pārvaldē un privātajā sektorā pastāv izpratne par apdraudējumiem un riskiem kibertelpā, ir spējas identificēt ļaunprātīgu rīcību un valstij ir tehniskie un cilvēku resursi, lai novērstu vai mazinātu naidīgas rīcības ietekmi.

Tīklu un informācijas sistēmu drošības direktīvas pieņemšana 2016. gada jūlijā bija liels solis virzībā uz kiberdrošības veicināšanu Eiropas līmenī. Direktīva paredz pirmos ES mēroga noteikumus par kiberdrošību, uzlabo kiberdrošības spējas un stiprina dalībvalstu sadarbību. Tā arī prasa kritiski svarīgo nozaru uzņēmumiem veikt attiecīgus drošības pasākumus un par visiem nopietniem kiberdrošības incidentiem ziņot attiecīgajai valsts iestādei. Savukārt 2016. gada jūlijā NATO atzina kibertelpu kā darbības vidi, kurā NATO ir jāaizstāv sevi tikpat efektīvi, kā tas notiek gaisā, uz sauszemes un jūrā. Savukārt 2018. gada Briseles samitā Alianse vienojās izveidot jaunu Kibertelpas operāciju centru kā daļu no NATO komandstruktūras. Latvija, kā NATO un ES dalībvalsts, aktīvi iesaistās kiberaizsardzības spēju attīstīšanā un kopējās mācībās.

Valstis turpina attīstīt ne tikai kiberaizsardzības, bet arī uzbrukuma spējas, kuras ir jāizmanto saskaņā ar starptautiskajām tiesībām. Latvija pamatnostādņu pārskata periodā savu spēju attīstībā koncentrēsies uz aizsardzības spēju attīstīšanu, vienlaikus neizslēdzot iespēju gan nacionāli, gan sadarbībā ar citām valstīm attīstīt un pilnveidot uzbrukuma rakstura kiberspējas.

## IKT izturētspēja[[3]](#footnote-4), sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana

Valsts atkarība no IKT infrastruktūras un elektroniskajiem pakalpojumiem ir pastāvīgi jāpārvalda un tai ir jāietver alternatīvu risinājumu sistēma, kas varētu tikt izmantota gadījumos, kad normāla IKT infrastruktūras un elektronisko pakalpojumu darbība nav iespējama vai ir traucēta.

IKT infrastruktūra ir jāaizsargā no draudiem un kritisko datu glabāšana un apstrādāšana ir jāveic drošos datu centros, izvērtējot iespējas kritisko datu kopijas uzglabāt arī ārpus Latvijas. Valsts, pašvaldību un vitāli svarīgu pakalpojumu darbībai nepieciešamās informācijas sistēmas ir jāizstrādā un jāpārvalda tā, ka tiek ņemti vērā drošības riski un paredzēti līdzekļi un pasākumi risku pārvaldīšanai. Līdzīgi, krīzes un kara laikā valdībai ir jānodrošina informācijas un kibertelpas aizsardzība, izmantojot aktīvus un pasīvus aizsardzības pasākumus, lai nepieļautu iedzīvotāju ārēju ietekmēšanu un valdības rīcības paralizēšanu.

Valsts un pašvaldību institūcijām un publisko elektronis­ko sakaru pakalpojumu sniedzējiem, kā arī IKT kritiskās infrastruktūras vadītājiem Informācijas tehnoloģiju drošī­bas likums un ar to saistītie Ministru kabineta noteikumi nosaka pamata drošības prasības, kuru realizācija ir pirmais solis drošas un uzticamas kibertelpas veidošanā, kurā ir garantēta valstij un sabiedrībai būtisku pakal­pojumu droša, uzticama un nepārtraukta saņemšana un sniegšana.

Plašāka sabiedrības iesaistīšanās digitālo resursu un pakalpojumu drošības veicināšanā var sniegt būtisku ieguldījumu valsts informācijas sistēmu izturētspējas uzlabošanā. Tādēļ, lai stiprinātu IKT drošību, kā arī veicinātu nepilnību un ievainojamību novēršanu un sistēmu veidotāju un turētāju atbildību, ir jāizstrādā regulējums atbildīgas drošības nepilnību atklāšanas procesam, kā to paredz Valsts aizsardzības koncepcija.

## Sabiedrības izpratne, izglītība un pētniecība

Cilvēka zināšanas un rīcība ir būtisks faktors jebkurā kiberdrošības programmā. Tāpēc kiberdrošība sākas ar izpratni, sākot no sistēmu un programmu izstrādātājiem līdz gala lietotājiem, kuri var saskarties gan ar pikšķerēšanas e‑pasta ziņojumiem, gan sociālās inženierijas uzbrukumiem. Rezultātā visiem iesaistītajiem ir būtiska loma tīklu un informācijas sistēmu drošības nodrošināšanā, un ir jāveicina gan izpratne par riskiem, ar kuriem iespējams saskarties tiešsaistē, gan spējas veikt darbības, lai pasargātu sevi no tiem. Kiberdrošības garantēšana ir kopīga atbildība, kur katra indivīda zināšanas, izpratne un vērība ir būtiska.

Latvijas izglītības sistēmai ir jābūt orientētai uz informācijas sabiedrības izveidošanu, jeb tādu sabiedrību, kuras locekļi prot, var un viņiem ir iespējas ar IKT palīdzību iegūt informāciju, saistīt to ar esošajām zināšanām un jau­niegūtās zināšanas izmantot savas labklājības celšanai.

Saskaņā ar Eiropas Komisijas 2018.gada digitālās ekonomikas un sabiedrības indeksu ziņojumu, Latvijā IKT speciālistu skaits veido vien 2,2% no visiem strādājošajiem, kas ir ievērojami zem ES vidējā līmeņa jeb 3,7%. Savukārt apmēram pusei valsts iedzīvotāju digitālo prasmju nav, vai arī tās ir zemā līmenī. Vienlaikus IKT jomā Latvijā ir arī relatīvi zema pētniecības intensitāte, ko apliecina Eiropas Komisijas Vienotā pētījumu centra 2017.gada ziņojums.

Ir kritiski svarīgi, lai sabiedrība apgūtu pamatprasmes iekārtu un programmatūras izmantošanā, kā arī ievērotu drošības pamatprincipus darbībai interneta vidē, kas veidotu pamatu nākamajiem zināšanu līmeņiem. Ņemot vērā situāciju, būtiska loma ir izglītībai un datorikas mācīšanai Latvijas skolās, kā arī IKT speciālistu sagatavošanai profesionālās vidējās un augstākās izglītības iestādēs. Pētniecības programmas ir nepieciešamas, lai attīstītu, gan eksperimentālās izstrādnes, gan, lai īstenotu valsts pasūtījumu, veidojot valsts pētījumu programmu “Kiberdrošība”.

Nozīmīga loma digitālo, tai skaitā kiberdrošības, tehnoloģiju attīstībā paredzēta ES daudzgadu budžeta plānā 2021.-2027. gadam. Ar mērķi veicināt ES globālo konkurētspēju digitālo tehnoloģiju jomā arī Latvija vairākās ES programmās varēs piesaistīt finansējumu projektiem, kas skar kiberdrošību.

Aizsardzības nozarē, lai veicinātu izpratni un sniegtu atbalstu moderno apdraudējumu situācijās, ir izveidotas speciālas vienības un nodrošināta apmācība kiberaizsardzības jautājumos gan Zemessardzē, gan Jaunsardzē, kā to paredz Valsts aizsardzības koncepcija.

## Starptautiskā sadarbība

Kibertelpa ar tās piedāvātajām iespējām un radītajiem drošības apdrau­dē­ju­miem nepazīst valstu nacionālās robežas, un tādēļ neviena valsts nevar viena pati efektīvi stāties pretī jaunajiem drošības izaicinājumiem.

Apzinoties kibertelpas pieaugošo nozīmi ikvienas sabiedrības dzīvē, kiber­dro­šī­ba kā būtisks jautājums ir iekļauts starpvalstu sadarbības un starptautisko orga­ni­zā­ciju darba kārtībā. Divpusējos un daudzpusējos formātos, nereti ie­sais­tot arī privāto sektoru, tiek apskatīts plašs jautā­ju­mu loks, ieskaitot cilvēk­tiesību ievērošanu virtuālajā vidē un kiber­no­ziedzības apkarošanu, kri­tis­kās infrastruktūras aizsardzību, atbildības noteikšanu par kiberuzbrukumiem un apdraudējuma novēršanu nacionā­lajai drošībai. Šādos apstākļos nenovēr­ša­mi saskaras atšķirīgas valstu intereses, un līdz šim starptautiskajai sabied­rī­bai nav izdevies panākt ievērojamu progresu vienotas izpratnes un pieejas vei­do­ša­nā. Latvijai, sadarbojoties ar līdzīgi domājošām valstīm, ir jāveicina glo­bā­la vie­nota izpratne par kibertelpu un starptautisko normu piemērošanu tajā.

Kiberdrošība ir nozīmīga valsts aizsardzības sastāvdaļa, un krīzes situācijā nacionāli attīstītās aizsardzības spējas var tikt stiprinātas arī ar sabiedroto NATO un ES valstu palīdzību. Lai nepieciešamības gadī­jumā efektīvi saņemtu un sniegtu atbalstu, kā arī lai stiprinātu kiberdro­šības pasākumus eiro­atlan­tis­ka­jā telpā, jāveicina gan šo organizāciju kolektīvo, gan katras dalībvalsts indivi­duālo kiberaizsardzības spēju attīstīšana atbilstoši pieņemtajiem NATO un ES kiberdrošības doku­men­tiem. Ņemot vērā kopīgos izaicinājumus, NATO un ES stiprina sadarbību kiberaizsardzības jomā, jo īpaši informācijas apmai­ņā, mācībās un pētniecībā. Latvija kā abu šo organizāciju dalībvalsts aktīvi iesaistās kiberaizsardzības aktivitāšu koordinācijā un mācībās.

Pamatnostādņu īstenošanas laikā Latvija starptautiskajā mērogā:

* stiprinās sadarbību ar līdzīgi domājošām valstīm, lai veicinātu vienotu valstu izpratni par kibertelpu;
* aktīvi līdzdarbosies NATO, ES, EDSO un ANO, lai veicinātu drošību kibertelpā un brīvības normu nostiprināšanu kiberdrošības politikā, kā arī stiprinātu IKT drošību un pieejamību;
* jēgpilni izmantos jau esošus starptautiskos instrumentus un mehā­nis­mus, lai aizsargātu kibertelpu no ļaunprātīgām aktivi­tātēm;
* turpinās atbalstīt starptautiskos centienus savstarpējas uzticē­ša­nās un sadarbības veicināšanai, uzsverot, ka spēkā esošajām starptautiskajām tiesību normām jābūt vienlīdz piemērojamām kā fiziskajā, tā virtuālajā vidē;
* turpinās Latvijā regulāri rīkot starptautiskus pasākumus kiberdrošības jomā, iezīmējot Latviju kā atbildīgu valsti, kas rūpējas par IKT drošību nacionālā un starptautiskā mērogā;
* turpinās sagatavot un pārbaudīt nacionālās procedūras, lai kiber­ap­draudējuma gadījumā ātri un efektīvi saņemtu palīdzību atbilstoši Latvijas un NATO saprašanās memorandam un saskaņā ar NATO Kiberdrošības koncepciju un Rīcības plānu;
* stiprinās kiberaizsardzības spējas, piedaloties dažādās starp­tau­tis­kās mācībās, vingrinājumos, kiberuzbrukumu simulācijā gan NATO un ES, gan citos valstu sadarbības mehānismos, dodot iespēju vietējiem speciālistiem un KAV pilnveidot zināšanas jau­nā­kajos informācijas sistēmu drošības risinājumos.

Nozīmīgs ieguldījums kiberdrošības starptautiskās sadarbības veicināšanā ir programmai Apvārsnis 2020. Jāatzīmē, ka 2021.gadā sāksies jaunā ietvarprogramma Apvārsnis Eiropa, kurā kiberdrošība būs būtiska komponente otrajā pīlārā, it īpaši tematiskajā kopā “Iekļaujoša un droša sabiedrība”, kur tas ir viens no šīs kopas rīcības virzieniem.

## Tiesiskums kibertelpā un kibernoziedzības mazināšana

Kibernoziegumu radītais jebkura veida kaitējums mazina uzticēšanos digitālajiem pakalpojumiem. Kibernoziedzības mazināšanai ir nepieciešama rīcība divos pamata virzienos – preventīvs darbs noziedzīgu darbību īstenošanas mazināšanai un efektīva noziedzības apkarošana. Vienlaikus jāuzsver arī sabiedrības līdzdalības aspekts, kas balstās sabiedrības izpratnē par kiberdrošību, jo plašāka sabiedrības izpratne par kiberdrošības riskiem palīdz novērst kibernoziegumus. Plašāka izpratne tiek panākta, kibernoziedzības problemātiku apskatot dažādos formātos (izglītības iestādes, pētnieciskie centri, konferences, utt.) un informējot cilvēkus, balstoties uz drošas uzvedības pētījumiem un analīzi.

Kibernoziedzības apkarošanu varētu atvieglot uzlabojot tiesībsargājošām iestādēm tehniskās iespējas identificēt interneta protokola adrese, no kurām ir veikta piekļuve noteiktiem e-pakalpojumiem vai informācijas resursiem. Šobrīd elektronisko sakaru komersanti IPv4 adrešu trūkuma dēļ aktīvi izmanto tīkla adrešu translēšanu un Latvijā viena IPv4 adrese tiek izmantota līdz pat 100 lietotājiem, kas rada dažādas problēmas, tai skaitā arī drošības jomā, jo tiesībsargājošās iestādes no saglabājamiem datiem ar grūtībām spēj identificēt galalietotāju, kurš ir veicis pretlikumīgas darbības. Risinājums šai problēmai ir uzsākt IPv6 ieviešanu valsts pārvaldē, tādējādi veicinot interesi par IPv6 ieviešanu arī privātajā sektorā.

# Turpmākā rīcība

Pamatnostādņu rīcības virzienu īstenošana ir atspoguļota 1.pielikumā un 2.pielikumā (informācijas dienesta vajadzībām) pievienotajā rīcības plānā, kurā norādīti:

* uzdevumi un pasākumi izvirzītā mērķa sasniegšanai;
* izpildes termiņš;
* atbildīgā institūcija;
* iesaistītās institūcijas;
* nepieciešamais finansējums un tā avoti;
* sasniedzamais rezultāts.

# Ietekmes novērtējums uz valsts budžetu un pašvaldību budžetu

Pamatnostādņu īstenošanai plānotie finanšu avoti ir valsts un pašvaldību budžets un ES fondu finanšu līdzekļi. Pamatnostādnēs noteikto rīcības virzienu finansēšanai var tikt piesaistīts arī privātais kapitāls, kas piesaistāms, veiksmīgi attīstot publiskās un privātās partnerattiecības, kā arī citus risinājumus privātā kapitāla piesaistei. Pamatnostādņu ietvaros noteikto uzdevumu un pasākumu izpildei nepieciešamais finansējums un tā iespējamie avoti ir norādīti 1.pielikumā un 2.pielikumā (informācija dienesta vajadzībām).

Pamatnostādņu paredzēto pasākumu īstenošana tiks nodrošināta pamatnostādnēs minētajām institūcijām piešķirto valsts budžeta un pašvaldību budžeta līdzekļu ietvaros. Jautājums par papildu valsts budžeta līdzekļu piešķiršanu pamatnostādnēs minētajām institūcijām izskatāms Ministru kabinetā gadskārtējā valsts budžeta likumprojekta sagatavošanas un izskatīšanas procesā.

1.tabula

**Politikas plānošanas dokumenta ietekme uz valsts un pašvaldību budžetiem**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Turpmākie trīs gadi (EUR) | | |
| 2019.gads | 2020.gads | 2021.gads |
| Kopējās izmaiņas budžeta ieņēmumos t.sk.: | 0 | 0 | 0 |
| Izmaiņas valsts budžeta ieņēmumos | 0 | 0 | 0 |
| Izmaiņas pašvaldību budžeta ieņēmumos | 0 | 0 | 0 |
| Kopējās izmaiņas budžeta izdevumos t.sk.: | 520 000 | 500 000 | 500 000 |
| Izmaiņas valsts budžeta izdevumos | 520 000 | 500 000 | 500 000 |
| Izmaiņas pašvaldību budžeta izdevumos | 0 | 0 | 0 |
| Kopējā finansiālā ietekme: | -520 000 | -500 000 | -500 000 |
| Finansiālā ietekme uz valsts budžetu | -520 000 | -500 000 | -500 000 |
| Finansiālā ietekme uz pašvaldību budžetu | 0 | 0 | 0 |
| Detalizēts ieņēmumu un izdevumu aprēķins (ja nepieciešams, detalizētu ieņēmumu un izdevumu aprēķinu pievieno politikas plānošanas dokumenta pielikumā. Ietekmi uz valsts un pašvaldību budžetiem norāda atsevišķi valsts un pašvaldību budžetam) | Tabulā ietverts tikai to pamatnostādņu 1.pielikuma uzdevumu un pasākumu īstenošanai nepieciešamais valsts budžeta finansējums, kuriem ir zināms nepieciešamā finansējuma apjoms.  Tabulā nav ietverts pamatnostādņu 2.pielikuma (informācija dienesta vajadzībām) uzdevumu un pasākumu īstenošanai nepieciešamais valsts budžeta finansējums.  Lēmums par pārējo pamatnostādņu rīcības plāna uzdevumu un pasākumu īstenošanai nepieciešamo valsts budžeta finansējumu tiks izskatīts Ministru kabinetā likumprojekta par valsts budžetu kārtējam gadam sagatavošanas gaitā. Nepieciešamā finansējuma detalizētus aprēķinus atbildīgās institūcijas veiks, gatavojot budžeta pieprasījumus kārtējam gadam vai iesniedzot jauno politikas iniciatīvu pieprasījumu attiecīgajam gadam. | | |
| Izmaiņas budžeta izdevumos 2022.gadā | 2022.gadā –  500 000 | - | - |

# Pārskatu iesniegšanas kārtība

Aizsardzības ministrija sadarbībā ar visām iesaistītajām institūcijām un NITDP līdz 2021.gada 1.martam iesniedz Ministru kabinetā informatīvo ziņojumu par pamatnostādņu rīcības plānā noteikto uzdevumu un pasākumu ieviešanas gaitu, bet līdz 2023.gada 1.jūnijam – informatīvo ziņojumu par pamatnostādņu rīcības plāna īstenošanas gala novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem.

# Noslēguma jautājumi

Piedāvātā risinājuma sākotnējais (*ex-ante*) ietekmes novērtējums nav veikts, jo kiberdrošība ir pastāvīgi un strauji evolucionējoša, bet pamatnostādnēs noteiktie rīcības virzieni ir iepriekš Nacionālās drošības koncepcijā noteikto prioritāšu un līdz šim uzsākto darbību turpinājums. Pamatnostādnēs paredzētais nacionālās kiberdrošības novērtējums veidos bāzi tālākas politikas un rīcības plāna izvērtēšanā un pilnveidošanā.

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

Aizsardzības ministrs Raimonds Bergmanis

22.11.2018 11:05

5247

G. Mezītis

67335350

gatis.mezitis@mod.gov.lv

1. Kiberdrošība pamatnostādņu izpratnē ir instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības, apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizēšanas un lietotāju resursu aizsardzībai. Or­ganizācija un lietotāju aktīvi ietver savienotas skaitļošanas tehnoloģijas, personālu, infrastruktūru, programmatūru, pakalpojumus, telekomunikāciju sistēmas un pārsūtītas jeb uzglabātas informācijas kopumu elektroniskajā vidē. Starptautiskās telekomunikāciju savienības definīcija angļu valodā: „Cybersecurity is the collection of tools, policies, security concepts, secu­rity safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructu­re, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.” ITU-T X.1205. [↑](#footnote-ref-2)
2. LI pamatnostādņu izpratnē ir fizisku objektu tīkls, kas izmanto sensorus un lietojumprogrammas saskarsmi, lai savienotos un apmainītos ar datiem interneta vidē. [↑](#footnote-ref-3)
3. IKT izturētspēja pamatnostādņu izpratnē ir IKT spēja izturēt, atgūties un mainīties ārējo traucējumu gadījumā, piemēram, kiberuzbrukuma vai dabas katastrofas gadījumā. [↑](#footnote-ref-4)