Informatīvais ziņojums
“Latvijas kiberdrošības stratēģija 2019.–2022. gadam”

Rīga, 2019

Saturs

Pielikums:

Rīcības virzienu uzdevumi (informācija dienesta vajadzībām)

Kopsavilkums

Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam" (turpmāk – Stratēģija) izstrādāta, pamatojoties uz Informācijas tehnoloģiju drošības likuma 11. panta otro daļu. Tā 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. Visaptverošā 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 tehnoloģiju (IT) drošības incidents).

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, Stratēģijā izvirzīti pieci rīcības virzieni 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 Stratēģijas 4. nodaļā, un katram no tiem ir izvirzīti uzdevumi, to izpildes termiņi, atbildīgās un iesaistītās institūcijas, nepieciešamie finanšu līdzekļi un sasniedzamais rezultāts, lai sasniegtu Stratēģijā definēto vīziju un mērķi. Rīcības virzienu uzdevumi, kas ietver informāciju dienesta vajadzībām, ir pieejami Stratēģijas pielikumā (informācija dienesta vajadzībām).

Stratēģijā aplūkotajā laika periodā atbildīgās un iesaistītās institūcijas turpinās realizēt iepriekšējā periodā iniciētos pastāvīgos uzdevumus, kā arī Stratēģijā definētie uzdevumi neierobežo institūcijas veikt citas neminētas darbības.

Atbildīgās institūcijas Stratēģijā paredzētos uzdevumus 2019. gadā īstenos piešķirto valsts budžeta līdzekļu ietvaros, savukārt jautājums par papildu valsts budžeta līdzekļu piešķiršanu 2020.–2022. 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
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
FM	Finanšu ministrija
IC	Iekšlietu ministrijas Informācijas centrs
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
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
MilCERT	Militāro 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
NVO	Nevalstiskās organizācijas
SAB	Satversmes aizsardzības birojs
SM	Satiksmes ministrija
SPRK	Sabiedrisko pakalpojumu regulēšanas komisija
Stratēģija	Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. 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
VRS	Valsts robežsardze
VRAA	Valsts reģionālās attīstības aģentūra
VSAA	Valsts sociālās apdrošināšanas aģentūra

Ievads

Stratēģija raksturo Latvijas kiberdrošības[1] situāciju, identificē nākotnes izaicinājumus un definē nacionālās kiberdrošības politikas rīcības virzienus laika periodam līdz 2022. gadam, tādējādi turpinot pamatnostādņu "Latvijas kiberdrošības stratēģija 2014–2018"[2] 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.

Stratēģija izstrādāta, pamatojoties uz Informācijas tehnoloģiju drošības likuma 11. panta otrajā daļā noteikto deleģējumu un 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.

---

[1] Kiberdrošība Stratēģijas 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.

[2] Apstiprinātas ar MK 2014. gada 21. janvāra rīkojumu Nr. 40.

1. Vīzija, mērķi, prioritātes un pamatprincipi

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.

Latvijai ir jāizmanto digitālās vides priekšrocības, lai nodrošinātu ekonomisko un sociālo labklājību, vienlaikus samazinot kiberdrošības risku vispārējo līmeni, nevajadzīgi neierobežojot tehnoloģiju, sakaru un datu plūsmu. Ir jānodrošina būtisku pakalpojumu sniegšana un saņemšana, kā arī kritiskās infrastruktūras darbība, aizsargājot indivīdus no kiberdrošības apdraudējumiem, vienlaikus ņemot vērā vajadzību aizsargāt valsts drošību, kā arī saglabāt cilvēktiesības un pamatvērtības.

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, ir 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 efektīvi reaģētu uz IKT drošības incidentiem, un nodrošinātu IKT aizsardzību un spēju funkcionēt. Sabiedrībai, privātajam un publiskajam sektoram ir jāattīsta zināšanas un spējas aizstāvēt sevi.

Atturēšana – atklāt, izmeklēt un pārtraukt ļaunprātīgas darbības kibertelpā, identificējot likumpārkāpējus un saucot 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 pamatprincipi ir šādi:

- kiberdrošība nav pašmērķis, bet gan neatņemama nacionālās drošības sastāvdaļa – mūsdienu valsts, sabiedrības un ekonomikas funkcionēšanas pamats;
- kiberdrošības veicināšana starptautiski, sadarbojoties ar sabiedrotajiem un partneriem, nepieciešama, lai sasniegtu nacionālos kiberdrošības mērķus;
- kiberdrošības jautājumu koordinācijā iesaistām pilsonisko sabiedrību, privātās, publiskās un akadēmiskās jomas pārstāvjus;
- kiberdrošība tiek nodrošināta, ievērojot arī cilvēktiesības;
- kiberuzbrukumu laicīga paredzēšana, izmeklēšana un novēršana ir svarīga;
- kiberdrošība sākas ar individuālu atbildību par drošu IKT izmantošanu.

2. Kiberdrošības pārvaldība

2.1. Risku pārvaldība

Mūsdienu valsts un sabiedrības funkcionēšana ir vitāli 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 ekonomisko un sociālo attīstību, nenodarītu zaudējumus ekonomikai un gūtu labumu no IKT gan valsts pārvaldē, gan privātajā sektorā.

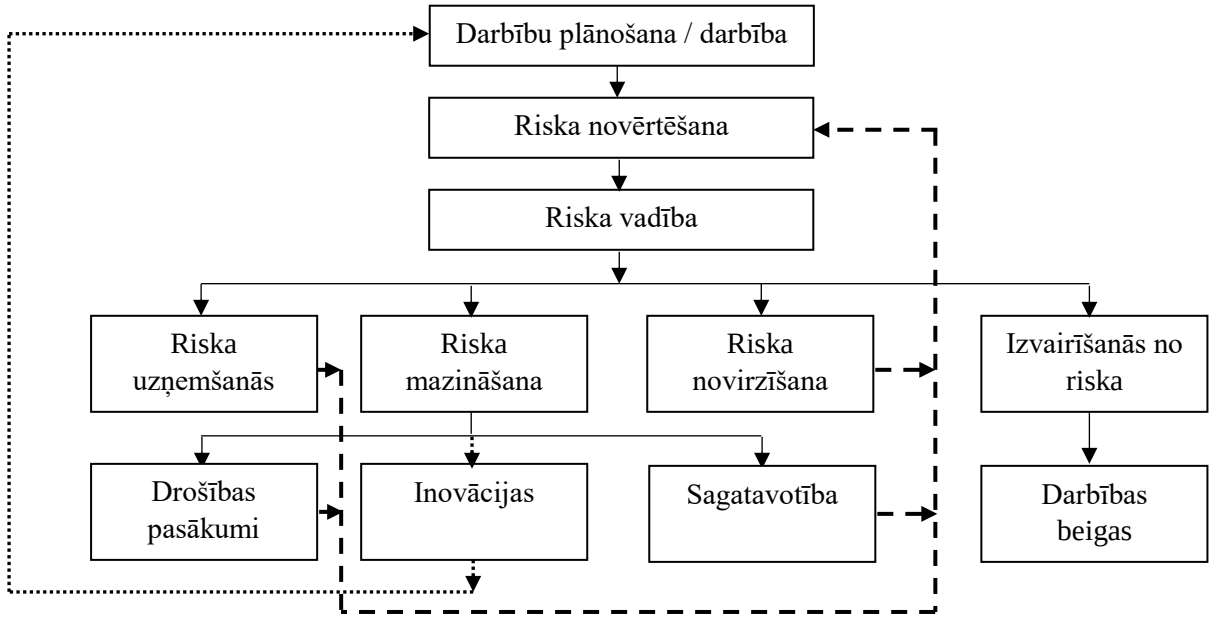
Ievērojot Ekonomiskās sadarbības un attīstības organizācijas (ESAO) rekomendācijas[3], visiem kiberdrošības pārvaldībā iesaistītajiem dalībniekiem ir jāievēro šādi četri vispārīgie kiberdrošības risku pārvaldības principi:

- saprast kiberdrošības riskus un to pārvaldību;
- uzņemties atbildību par kiberdrošības risku pārvaldību;
- pārvarēt kiberdrošības riskus pārredzamā veidā un saskaņā ar cilvēktiesībām un pamatvērtībām;
- sadarboties, tostarp starptautiskā līmenī.

Kiberdrošības risku pārvaldība ir neatņemama lēmumu pieņemšanas procesa daļa, kas saistīta ar darbību plānošanu un veikšanu visā šo darbību dzīvescikla laikā. Kiberdrošības risku pārvaldība sastāv no riska novērtēšanas un vadības, uzņemoties, mazinot vai novirzot kiberdrošības risku vai izvairoties no riska (sk. 1. shēmu). Stratēģijā aprakstīto kiberdrošības risku pārvaldības shēmu kiberdrošībā iesaistītie dalībnieki var izmantot par pamatu, izstrādājot savas organizācijas iekšējo risku pārvaldības shēmas. Iesaistītā institūcija riska mazināšanai var izmantot gan atbilstošus un proporcionāli riskam izvēlētus drošības pasākumus, gan apsvērt jauninājumus saistībā gan ar drošības pasākumiem, gan attiecīgo darbību, kā arī var noteikt un piemērot sagatavotības pasākumus, tādējādi elastīgi reaģējot uz negadījumu un nodrošinot darbības nepārtrauktību.

1. shēma

Kiberdrošības risku pārvaldības shēma



Avots: ESAO rekomendācijas "Digital Security Risk Management for Economic and Social Prosperity" (2015)

Stratēģijā, nosakot kiberdrošības politikas rīcības virzienus un ar tiem saistītos uzdevumus, galvenais uzsvars tiek likts, pirmkārt, uz četru vispārīgo kiberdrošības risku pārvaldības principu pilnveidošanu, īpaši to izvēršot rīcības virzienos: a) sabiedrības izpratne, izglītība un pētniecība, b) starptautiskā sadarbība, un, otrkārt, risku mazināšanu, kam veltīti divi kiberdrošības politikas rīcības virzieni: a) kiberdrošības veicināšana, digitālās drošības risku mazināšana, b) IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana.

[3] ESAO rekomendācijas "Digital Security Risk Management for Economic and Social Prosperity" (2015)

2.2. Pārvaldības modelis un iesaistīto dalībnieku funkcijas un pienākumi

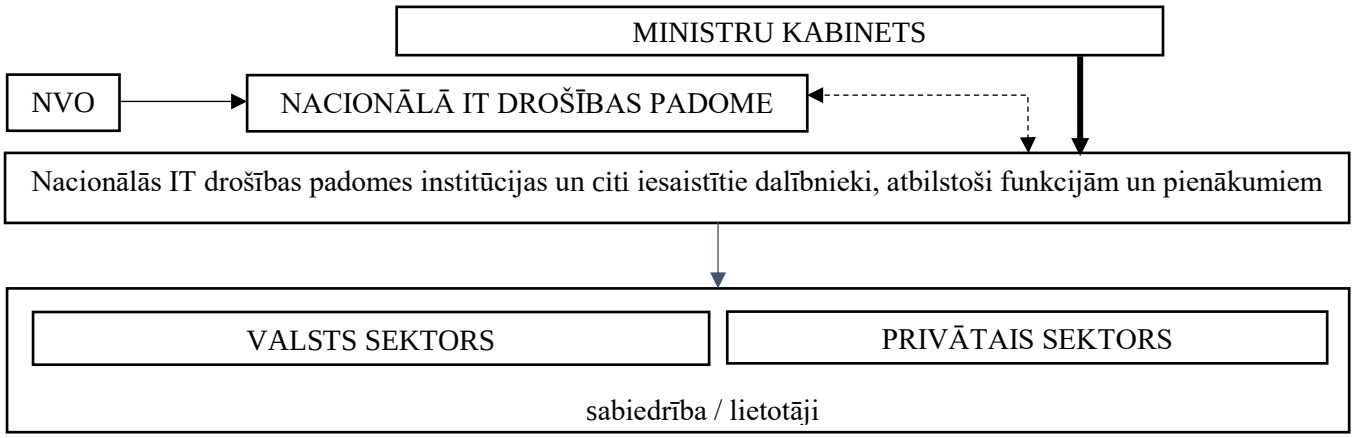
Kiberdrošības pārvaldības jomā Latvijā tiek īstenots daļēji centralizēts pārvaldības modelis, kur vadošās iestādes plāno kiberdrošības Stratēģiju un koordinē un īsteno tajā paredzētos uzdevumus, katrai iestādei savas kompetences jautājumos nodrošinot paredzēto uzdevumu praktisku ieviešanu un izpildi. Nacionālās kiberdrošības pārvaldības pamatā ir savstarpējā sadarbība, kur, katrai valsts iestādei pildot savas funkcijas, tajā skaitā kibertelpā, tiek īstenota tieša sadarbība ar citām iestādēm un privāto sektoru vai sadarbība Nacionālās informācijas tehnoloģiju drošības padomē[4] (NITDP) (sk. 2. shēmu).

NITDP ir izveidota, pamatojoties uz Informācijas tehnoloģiju drošības likumu, kas nosaka kiberdrošības politikas veidošanu nacionālajā līmenī un uzdod NITDP koordinēt kiberdrošības politikas izstrādi, uzdevumu 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 (AM).

Digitālās drošības uzraudzības komiteja (DDUK) savukārt ir koleģiāla uzraudzības institūcija aizsardzības ministra pakļautībā, kuras mērķis ir uzraudzīt un reģistrēt kvalificētus vai kvalificētus paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzējus un to sniegtos pakalpojumus kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju reģistrā. DDUK veic Fizisko personu elektroniskās identifikācijas likumā noteiktās uzraudzības institūcijas funkcijas un uzdevumus, kā arī paziņo Eiropas Komisijai elektroniskās identifikācijas shēmas, sagatavo priekšlikumus attiecībā uz normatīvo aktu projektiem par kvalificētu vai kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju un tā sniegto pakalpojumu uzraudzību, kā arī savas kompetences ietvaros sniedz priekšlikumus valsts un pašvaldības iestādēm.

2. shēma

Kiberdrošības pārvaldības modelis



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

- Aizsardzības ministrija (AM) 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.

[4] MK 2016. gada 1. novembra noteikumi Nr. 695 "Digitālās drošības uzraudzības komitejas nolikums"

AIMZino_080819_IZLKS; Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.-2022.gadam"

- Ārlietu ministrija (ĀM) koordinē starptautisko sadarbību un Latvijas dalību dažādās ar kiberdrošību saistītās starptautiskās iniciatīvās.
- Datu valsts inspekcija (DVI) pilda ES Regulā 2016/679 (2016. gada 27. aprīlis) "Par fizisku personu datu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK" un Fizisko personu datu apstrādes likumā noteiktos uzdevumus datu apstrādes jomā.
- Ekonomikas ministrija (EM) izstrādā ekonomikas politiku un veicina konkurētspējas un inovāciju attīstību.
- 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.
- 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.
- 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 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.
- 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 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 informācijas tehnoloģiju drošības incidentu novēršanas komanda (MilCERT) nodrošina AM 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.
- 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 IT 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 un autentifikācijas rīku darbībai nepieciešamo infrastruktūru.
- Valsts drošības dienests (VDD) īsteno valsts (un sabiedrības) iekšējās drošības uzraudzību.
- 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.

Visas valsts un pašvaldību institūcijas, kā arī IT kritiskās infrastruktūras (KI) īpašnieki vai tiesiskie valdītāji savā darbībā ievēro Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" prasības.

3. Kiberdrošības situācijas analīze

3.1. Situācijas raksturojums

Lai mazinātu kibertelpā esošo draudu iespējas ietekmēt informācijas sistēmu darbību, kiberuzbrukumu izplatību un sekas, Latvijai ir jāturpina 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. Jāņem 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 sistēmu drošības direktīvas[5] mērķi – izlīdzināt un stiprināt ES dalībvalstu kiberdrošības spējas, ņemot vērā Latvijas ģeogrāfisko atrašanās vietu un saistības ar 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 nodarītos zaudējumus vismaz 265 miljardus *euro* apmērā 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 – kiberuzbrukumi pieaug valsts pārvaldes iestādēs, izmantojot pikšķerēšanas (*phishing*), izspiedējvīrusu (*ransomware*) un ļaunatūras (*malware*) augšuplādes uzbrukumu metodes, datu izgūšanu vai integritātes kompromitēšanu.

Iejaukšanās citu valstu vēlēšanu kampaņās, izmantojot dažādus līdzekļus sociālajos tīklos, daudzviet ir kļuvusi par nacionālās drošības jautājumu. Vēlēšanu drošības koordinācijas

[5] Eiropas Parlamenta un Padomes 2016. gada 6. jūlija direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā

grupas izveide ir veids kā, apvienojot institūciju resursus, ir iespējams sagatavoties iespējamiem informācijas telpas apdraudējumiem pirms vēlēšanām.

Latvijas kibertelpa turpina saskarties ar plaša mēroga 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, kuru mērķis ir 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"[6], 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 spēju paredzēt un atvairīt kiberuzbrukumus ar neparedzētiem uzbrukuma raksturlielumiem un uzlabotu spēju 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 regulāri lieto internetbanku pakalpojumus (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. Preces vai pakalpojumus tiešsaistē iegādājušies 55% iedzīvotāju, un pakāpeniski pieaug mazo un vidējo uzņēmēju skaits, kuri 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 iestādēs.

Minētie rādītāji liecina par digitālās 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 vērsta pret valsts pārvaldes IKT sistēmām. IT drošības incidentu novēršanas institūcija (CERT.LV) kopš 2017. gada ir novērojusi šifrējošo izspiedējvīrusu lietojuma pieaugumu uzbrukumos valsts pārvaldes vai valstij kritiski svarīgām informācijas sistēmām, kas pasaules uzmanību piesaistīja *WannaCry* un *NotPetya* kiberuzbrukumu kampaņu laikā 2017. gada maijā un jūnijā. Šeit gan jāatzīmē, ka cietušo skaits Latvijā bija neliels un neviens no tiem nebija saistīts ar valsts sektoru vai kritisko infrastruktūru.

Kibertelpā tiek novēroti regulāri informācijas sistēmu un mājaslapu uzlaušanas mēģinājumi, krāpniecisko e-pastu kampaņas, kuru mērķis ir izkrāpt personu un autentifikācijas datus vai inficēt informācijas sistēmu ar ļaunatūru. Ļoti bieži datu noplūdes un sistēmu uzlaušanas iemesli ir nepietiekami droši konfigurētas lietotāju informācijas sistēmas un

[6] MK 2016. gada 29. martā skatīja informatīvo ziņojumu "Par pamatnostādņu "Latvijas kiberdrošības stratēģija 2014.-2018. gadam" rīcības plānojumā noteikto uzdevumu izpildes gaitu" (prot. 15 34. §). Saskaņā ar pamatnostādnēm "Par pamatnostādņu "Latvijas kiberdrošības stratēģija 2014.-2018. gadam" AIM sadarbībā ar visām iesaistītajām ministrijām un NITDP līdz 2019. gada 1. jūnijam iesniedz informatīvo ziņojumu par pamatnostādņu rīcības plāna īstenošanas gala novērtējumu

nepietiekamas zināšanas par drošu IKT risinājumu un digitālo tehnoloģiju lietošanu. 2018. gada 4. ceturksnī kopumā tika konstatētas 203 455 apdraudētas IP adreses, no kurām 131 394 tika atklātas konfigurācijas nepilnības, kuras kiberuzbrucēji varētu izmantot uzbrukumos. Plaši novērojama arī ļaundabīgā koda izplatība un ielaušanās mēģinājumi informācijas sistēmās, izmantojot lietotāju informācijas sistēmu ievainojamību un pakļaujot tās robotu tīklu turpmākajām ļaunprātīgajām darbībām.

3.2. 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 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 kopējā 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. 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 veicināt hakeru aktivitātes pieaugumu.

Kā viens no nākotnes izaicinājumiem ir jāmin arī lietu internets[7] (LI), jo, turpinot attīstīties arvien jaudīgākām datu pārraides tehnoloģijām, kuras var integrēt saimniecībās plaši izmantotas preces, ir vērojams LI popularitātes pieaugums, kura 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.

Mākoņdatošana un tās piedāvātie risinājumi, kuru strauja attīstība iesākās pirms vairākiem gadiem, neapšaubāmi, turpinās attīstīties, un šie risinājumi kļūs arvien populārāki. Līdztekus mākoņdatošanas tehnoloģisko iespēju attīstībai ir jāturpinās arī mākoņdatošanas drošības politikai (1. rīcības virziens, 1.1. uzdevums), kas attiecībā uz mākoņdatošanu vienmēr ir bijis sensitīvākais jautājums.

Mobilie tālruņi vairs nav tikai savstarpējās saziņas ierīces. Ja tālrunis tiek uzlauzts, citas tam pievienotās ierīces var būt nākamās, jo kopējā drošība ir tikpat spēcīga kā vājākais savienojums ierīču ķēdē. Lai paaugstinātu institūciju kiberdrošību, nepieciešams izvērtēt mobilo tālruņu un viedierīču lietošanas ierobežojumus, atrodoties institūcijas telpās, lai tādējādi pasargātu institūcijas IKT sistēmas no inficēšanās draudiem (rīcības virziens Nr. 1, 1.2. uzdevums.

Attīstoties Latvijas ekonomikai, arvien vairāk izjūtams dažādu jomu, sevišķi IKT, speciālistu trūkums, kas gan nav tikai Latvijas fenomens, bet izteikta situācija arī citviet pasaulē. Kvalificētu darbinieku trūkums noved pie nesamērīgi augstas uzņēmēju savstarpējās

[7] Lietu internets Stratēģijas izpratnē ir fizisku objektu tīkls, kas izmanto sensorus un lietojumprogrammas saskarsmi, lai savienotos un apmainītos ar datiem interneta vidē.

konkurences IKT speciālistu piesaistīšanā un, salīdzinot ar publisko sektoru, neproporcionāli augstas piedāvātās darba samaksas 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 (1. rīcības virziens, 1.4. uzdevums).

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

4. Nacionālās kiberdrošības politikas rīcības virzieni

Definējot nacionālās kiberdrošības politikas rīcības virzienus līdz 2022. gadam, jāņem vērā nacionālie politikas plānošanas un citi dokumenti un tajos izvirzītie kiberdrošības politikas ilgtermiņa mērķi. Šī sasaiste ir būtiska, lai nodrošinātu konsekventu kiberdrošības politikas attīstību. Vienlaikus šajā Stratēģijā nav iekļauti citos Ministru kabineta apstiprinātajos dokumentos iekļautie uzdevumi, lai neapgrūtinātu pieņemto lēmumu uzraudzību.

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.

Vienlaikus ES Tīklu un informācijas sistēmu drošības direktīvas 7. pants nosaka septiņus jautājumus, kuri dalībvalstīm jāievēro, īstenojot valsts tīklu un informācijas sistēmu drošības stratēģiju. Latvija, izstrādājot Stratēģiju laika periodam līdz 2022. gadam, ir iekļāvusi direktīvā izvirzītos jautājumus Stratēģijas nodaļās, tādējādi izpildot direktīvas prasības.

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 starptautiskās kibertelpas politikas izveide ES un ES pamatvērtību popularizēšana.

Ņemot vērā ES izvirzītās prioritātes un nacionālajos politikas plānošanas un citos dokumentos noteiktos mērķus, Stratēģijā ir izvirzīti pieci rīcības virzieni periodam līdz 2022. gadam:

1) kiberdrošības veicināšana, digitālās drošības risku mazināšana,
2) IKT izturētspēja[8], sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana,
3) sabiedrības izpratne, izglītība un pētniecība,

[8] IKT izturētspēja Stratēģijas izpratnē ir IKT spēja izturēt, atgūties un mainīties ārējo traucējumu gadījumā, piemēram, kiberuzbrukuma vai dabas katastrofas gadījumā.

4) starptautiskā sadarbība,
5) tiesiskums kibertelpā un kibernoziedzības mazināšana.

Visi iepriekšminētie rīcības virzieni ir detalizēti aprakstīti šīs nodaļas apakšnodaļās, un katram no tiem ir izvirzīti uzdevumi, to izpildes termiņi, atbildīgās[9] un iesaistītās institūcijas, nepieciešamie finanšu līdzekļi un sasniedzamais rezultāts, lai sasniegtu Stratēģijā definēto vīziju un mērķi. Sasniedzamie rezultāti ir laši un vispārīgi, ņemot vērā kiberdrošības komplekso dabu un straujo mainību. Rīcības virzienu uzdevumi, kas ietver informāciju dienesta vajadzībām, ir pieejami Stratēģijas pielikumā (informācija dienesta vajadzībām).

Stratēģijā aplūkotajā laika periodā atbildīgās un iesaistītās institūcijas turpinās realizēt iepriekšējā periodā iniciētos pastāvīgos uzdevumus, kā arī Stratēģijā definētie uzdevumi neierobežo institūcijas veikt citas neminētas darbības.

4.1. 1. rīcības virziens "Kiberdrošības veicināšana, digitālās drošības risku mazināšana"

Valsts mērķis ir visaptverošas valsts aizsardzības sistēmas izveide, kuru īstenojot, 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 identificēt ļaunprātīgu rīcību un efektīvi jāsadarbojas, nodrošinot valsts pārvaldē un privātajā sektorā izpratni par apdraudējumiem un riskiem kibertelpā, un valstij ir jārod tehniskie un cilvēkresursi, lai novērstu vai mazinātu naidīgas rīcības ietekmi. Krīzes vadības mācības, iesaistot tajās valsts drošības iestādes, valsts institūcijas un privāto sektoru, ir veids. kā attīstīt savstarpējo izpratni un koordinētu darbību krīzes situāciju pārvarēšanā (1.5. uzdevums).

Tīklu un informācijas sistēmu drošības direktīvas pieņemšana 2016. gada jūlijā bija liels solis kiberdrošības veicināšanā Eiropas līmenī. Direktīva paredz pirmos ES mēroga noteikumus kiberdrošībā, uzlabo kiberdrošības spējas un stiprina dalībvalstu sadarbību. Tā prasa vitāli svarīgo nozaru uzņēmumiem veikt attiecīgus drošības pasākumus un par nopietniem kiberdrošības incidentiem ziņot attiecīgajai Informācijas tehnoloģiju drošības incidentu novēršanas institūcijai. Savukārt 2016. gada jūlijā NATO ir atzinusi kibertelpu kā darbības vidi, kurā NATO jāaizstāv sevi tikpat efektīvi, kā tas notiek gaisā, uz sauszemes un jūrā. 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, un tas notiek saskaņā ar starptautiskajām tiesībām. Latvija Stratēģijas pārskata periodā savu spēju attīstībā koncentrēsies uz aizsardzības spēju attīstīšanu, vienlaikus neizslēdzot iespēju gan nacionāli, gan sadarbībā ar citām valstīm attīstīt un pilnveidot uzbrukuma kiberspējas.

Valsts un pašvaldību institūcijas Stratēģijas pārskata periodā turpinās attīstīt publisko pakalpojumu elektronisko pieejamību (e-pakalpojumus), jo tie būtiski paaugstina valsts un pašvaldību institūciju, sabiedrības un privātā sektora sadarbības efektivitāti. Vienlaikus ar iepriekšminēto procesu nepieciešams izstrādāt vienotus kritērijus, ar kādām autentifikācijas metodēm iespējams piekļūt konkrētajam e-pakalpojumam (1.3. uzdevums).

[9] Ja tabulas ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu.

1. tabula

1. rīcības virziena "Kiberdrošības veicināšana, digitālās drošības risku mazināšana" uzdevumi

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[10]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
1.1.	Definēt prasības, kas jānodrošina, izmantojot mākoņdatošanas pakalpojumus un ierobežojumus valsts pārvaldes un pašvaldību iestādēs	2020. g. 4. cet.	VARAM, AM, valsts drošības iestādes	CERT.LV, LPS	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Definētas prasības datu glabāšanai mākonī
1.2.	Veikt analīzi un, ja nepieciešams, noteikt mobilo tālruņu un viedierīču lietošanas un tīklu piekļuves tiesību ierobežojumus, atrodoties iestādes telpās un izmantojot iestādes pārziņā esošus informācijas resursus	2020. g. 4. cet.	Visas valsts pārvaldes institūcijas		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. Pašvaldības un pašvaldību iestādes uzdevumu realizē, ja iespējams, plānojot uzdevuma realizācijai nepieciešamos finanšu līdzekļus pašvaldību un pašvaldību iestāžu budžetu izstrādes laikā.	Veikta analīze un noteikti ierobežojumi
1.3.	Izstrādāt ieteikumus un kritērijus, ar kādu autentifikācijas metodi (eID, i-bankas autorizācija) ir iespējams piekļūt konkrētajam resursam	2019. g. 4. cet.	AM, VARAM		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. Pašvaldības un pašvaldību iestādes uzdevumu realizē, ja	Sagatavoti ieteikumi, apstiprināti kritēriji

[10] Ja ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[10]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
					iespējams, plānojot uzdevuma realizācijai nepieciešamos finanšu līdzekļus pašvaldību un pašvaldību iestāžu budžetu izstrādes laikā, vienlaikus ievērojot Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" prasības.	
1.4.	Veikt analīzi un izstrādāt rekomendācijas, kā veicināt IT speciālistu piesaisti valsts un pašvaldību iestādēm	2019. g. 4. cet.	VK, VARAM		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Analīze par veidiem, kā veicināt IT speciālistu piesaisti publiskā sektora amatos
1.5.	Reizi divos gados organizēt kiberdrošības krīzes vadības mācības, lai attīstītu savstarpējo sapratni un koordinētu darbību krīzes situāciju pārvarēšanā.	Pastāvīgi	AM, CERT.LV	Valsts pārvaldes un pašvaldību institūcijas un komersanti saskaņā ar mācību scenāriju	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Paaugstināta savstarpējā sapratne un darbību koordinācija krīzes situāciju pārvarēšanā

4.2. 2. rīcības virziens "IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana"

Valsts atkarība no IKT infrastruktūras un elektroniskajiem pakalpojumiem ir pastāvīgi jāpārvalda, un tai jāietver alternatīvu risinājumu sistēma, ko varētu izmantot gadījumos, ja 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 jāizstrādā un jāpārvalda, ņemot vērā drošības riskus un paredzētos līdzekļus un pasākumus risku pārvaldīšanai (2.3. uzdevums). 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 (2.2. uzdevums).

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

Plašāka sabiedrības iesaiste digitālo resursu un pakalpojumu drošības veicināšanā var sniegt būtisku ieguldījumu valsts informācijas sistēmu izturētspējas uzlabošanā. Tādēļ, lai stiprinātu IKT drošību, novērstu nepilnības un ievainojamības un vairotu sistēmu veidotāju un turētāju atbildību, ir jāizstrādā atbildīga drošības nepilnību atklāšanas procesa regulējums, kā to paredz Valsts aizsardzības koncepcija (2.1. uzdevums).

2. tabula

2. rīcības virziena "IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana" uzdevumi

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[11]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
2.1.	Izstrādāt normatīvo aktu bāzi, kas nosaka atbildīgu ievainojamību atklāšanas politiku	2021.g. 4.cet.	AM	CERT.LV, MilCERT, IeM (VP), VDD, TM (DVI), SM, VARAM, MIDD, SAB	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Sagatavota normatīvo aktu bāze
2.2.	Turpināt IKT izturētspējas stiprināšanu Latvijas pārstāvniecībās ārvalstīs	Pastāvīgi	ĀM		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Veikti pasākumi Latvijas pārstāvniecību ārvalstīs IKT izturētspējas stiprināšanai

[11] Ja ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[11]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
2.3.	CERT.LV organizēti valsts IKT risinājumu un infrastruktūras ielaušanās testi	Pastāvīgi	CERT.LV	NBS, KAV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Regulāri organizēti IKT risinājumu un infrastruktūras ielaušanās testi.

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

Cilvēka zināšanas un rīcība ir būtiski faktori jebkurā kiberdrošības programmā. Tāpēc kiberdrošība vispirms sākas ar izpratni par to, 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, tādēļ jāveicina izpratne gan par riskiem, ar kuriem iespējams saskarties tiešsaistē, gan spējas veikt darbības, lai pasargātu sevi. Garantijas kiberdrošības jomā ir saistītas ar kopīgu atbildību, kur katra indivīda zināšanas, izpratne un vērīgums ir svarīgi.

Latvijas izglītības sistēma ir orientēta uz informācijas sabiedrības veidošanu. Tā ir sabiedrība, kura prot, var un tai ir iespējas ar IKT palīdzību iegūt informāciju, saistīt to ar esošajām zināšanām un jauniegūtās zināšanas izmantot savai labklājībai. Vienlaikus centieniem paaugstināt sabiedrības vispārējās zināšanas ir jāveicina jauno IT speciālistu izglītošana un izaugsme, kur būtiska nozīme ir iespējām piedalīties interešu izglītības pasākumos un sacensībās kiberdrošības jomā (3.5. uzdevums).

Saskaņā ar Eiropas Komisijas 2018. gada ziņojumu "Digitālās ekonomikas un sabiedrības indekss" 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 vitāli svarīgi, lai sabiedrība apgūtu iekārtu un programmatūras izmantošanas pamatprasmes, kā arī ievērotu drošības pamatprincipus darbībai interneta vidē – tas veidotu pamatu nākamajiem zināšanu līmeņiem (3.2., 3.3. un 3.4. uzdevums). Ņemot vērā situāciju, būtiska loma ir izglītībai un datorikas mācīšanai Latvijas skolās, kā arī IKT speciālistu sagatavošanai profesionālajās vidējās izglītības un augstākās izglītības iestādēs. Lai veicinātu jauniešu interesi par IT, nepieciešams atbalstīt Latvijas dalību bērnu un jauniešu interešu izglītības pasākumos un sacensībās (3.5. uzdevums). Atbalsts pētniecībai vajadzīgs, lai attīstītu gan eksperimentālās izstrādnes, gan īstenotu valsts pasūtījumu. Lai veicinātu pētniecības attīstību kiberdrošības jomā par aktuāliem kiberdrošības jautājumiem, jāizmanto visi pieejamie atbalsta veidi: gan grantu projektu programmas, gan iepirkumi, gan atbalstot starptautiskās sadarbības projektus, piemēram, Eiropas aizsardzības fonda ietvaros, gan, pēc padziļinātas analīzes veikšanas, ja tiek identificēta nepieciešamība, iekļaujot sadaļu par kiberdrošību aizsardzības jomas valsts pētījumu programmā (3.1. uzdevums).

Nozīmīga loma digitālo, tai skaitā kiberdrošības, tehnoloģiju attīstībai paredzēta ES daudzgadu budžeta plānā 2021.–2027. gadam. Tās mērķis ir veicināt ES globālo konkurētspēju digitālo tehnoloģiju jomā. Arī Latvija vairākās ES programmās varēs piesaistīt finansējumu projektiem, kas saistīti ar 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.

3. tabula

3. rīcības virziena "Sabiedrības izpratne, izglītība un pētniecība" uzdevumi

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[12]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
3.1.	Sniegt atbalstu pētniecības attīstībai kiberdrošības jomā par aktuāliem kiberdrošības jautājumiem, izmantojot visus pieejamos atbalsta veidus.	Pastāvīgi	AM	IZM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Sniegts atbalsts pētniekiem atbilstoši pieejamajiem atbalsta veidiem un veicināta pētniecība par aktuāliem kiberdrošības jautājumiem. Sadarbībā ar IZM un atbilstošām pētniecības iestādēm veikta padziļināta analīze par valsts pētījumu programmas aizsardzības jomā izveidi, tajā ietverot sadaļu par kiberdrošību.
3.2.	Izglītojamo un pedagogu izpratnes veicināšana par informācijas drošību, privātuma aizsardzību un uzticamu e-pakalpojumu lietošanu.	Pastāvīgi	Valsts un pašvaldību izglītības iestādes (izņemot pirmsskolas izglītības iestādes), pašvaldības	IZM LIA	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. Pašvaldības un pašvaldību iestādes uzdevumu realizē, ja iespējams, plānojot	Paaugstināta audzēkņu, studentu un pedagogu izpratne par kiberdrošību

[12] Ja ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[12]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
					uzdevuma realizācijai nepieciešamos finanšu līdzekļus pašvaldību un pašvaldību iestāžu budžetu izstrādes laikā.	
3.3.	Stiprināt sabiedrības izpratni par drošu interneta lietošanu (izstrādāt izglītojošus un informatīvus materiālus dažādām vecuma grupām ar rekomendācijām par drošības pasākumiem, lietojot internetu, organizējot sociālās kampaņas) un organizēt atsevišķas sabiedrības daļas padziļinātu izglītošanu par kiberdrošības jautājumiem. Izstrādāt un īstenot ikgadēju starpinstitūciju darba un pasākumu plānu sabiedrības informēšanai un izpratnes veidošanai par kiberdrošības jautājumiem	Pastāvīgi	IeM (VP), IZM, AM, CERT.LV	KM, LIKTA, LIA, LFNA,	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Paaugstināta sabiedrības izpratne par drošību internetā
3.4.	Veicināt valsts un pašvaldību iestāžu darbinieku izpratni par drošu IKT lietošanu	Pastāvīgi	Visas valsts pārvaldes institūcijas, pašvaldības		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. Pašvaldības un pašvaldību iestādes uzdevumu realizē, ja iespējams, plānojot uzdevuma realizācijai nepieciešamos finanšu līdzekļus pašvaldību un pašvaldību iestāžu budžetu izstrādes laikā.	Paaugstināta valsts un pašvaldību darbinieku izpratne par drošu IKT lietošanu

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[12]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
3.5.	Veicināt atbalstu Latvijas dalībai bērnu un jauniešu interešu izglītības pasākumos un sacensībās kiberdrošības jomā	Pastāvīgi	IZM	VARAM, pašvaldības	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Latvijas bērni un jaunieši katru gadu piedalās vismaz vienā interešu izglītības pasākumā un / vai sacensībās kiberdrošības jomā

4.4. 4. rīcības virziens "Starptautiskā sadarbība"

Kibertelpa ar tās piedāvātajām iespējām un radītajiem drošības apdraudējumiem nepazīst valstu nacionālās robežas, 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 aplūkots 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 saņemtu un sniegtu efektīvu atbalstu un stiprinātu kiberdrošības pasākumus eiroatlantiskajā telpā, jāattīsta gan šo organizāciju kolektīvās, gan katras dalībvalsts individuālās kiberaizsardzības spējas 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 pasākumu koordinēšanā un mācībās. Stratēģijas īstenošanas laikā Latvija starptautiskajā mērogā:

- stiprinās sadarbību ar līdzīgi domājošām valstīm, lai veicinātu vienotu valstu izpratni par kibertelpu (4.1. uzdevums);
- aktīvi līdzdarbosies NATO, ES, EDSO, ANO un ESAO, lai veicinātu drošību kibertelpā un brīvības normu nostiprināšanu kiberdrošības politikā, kā arī stiprinātu IKT drošību un pieejamību (4.1. un 4.5. uzdevums);
- jēgpilni izmantos jau esošus starptautiskos instrumentus un mehānismus, lai aizsargātu kibertelpu no ļaunprātīgām darbībām (4.3. uzdevums);
- turpinās atbalstīt starptautiskos centienus, tostarp privātā sektora, savstarpējas uzticēšanās un sadarbības veicināšanai, uzsverot, ka spēkā esošajām starptautiskajām

tiesību normām jābūt vienlīdz piemērojamām kā fiziskajā, tā virtuālajā vidē (4.1. un 4.4. uzdevums);
- turpinās Latvijā regulāri rīkot starptautiskus pasākumus kiberdrošības jomā, reprezentējot 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 (4.2. uzdevums);
- stiprinās kiberaizsardzības spējas, piedaloties dažādās starptautiskajās 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 (4.2. uzdevums).

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

4. tabula

4. rīcības virziena "Starptautiskā sadarbība" uzdevumi

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[13]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
4.1.	Latvijas interešu formulēšana un aizstāvēšana, iesaistīšanās starptautiskās sadarbības iniciatīvās un platformās, sadarbības stiprināšana ar Baltijas un Ziemeļeiropas reģiona valstīm un aktīva līdzdalība NATO un ES iniciatīvās, tai skaitā atbalsta sniegšanā partnervalstu kiberdrošības spēju stiprināšanai. Aktīva līdzdalība formālas un neformālas sadarbības iniciatīvās un starptautisko organizāciju (ANO, EDSO) procesos	Pastāvīgi	ĀM, AM	Visas valsts pārvaldes institūcijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Nodrošināta pastāvīga un efektīva iesaiste starptautiskajos procesos. Vismaz reizi gadā organizētas kiberdrošības ekspertu konsultācijas. Regulāra Latvijas pārstāvja dalība starptautiskajās iniciatīvās un platformās.
4.2.	Dalība starptautiskajās kiberdrošības mācībās, kiberdrošības ekspertu un	Pastāvīgi	AM	ĀM, SM, IeM, CERT.LV,	Likumā par valsts budžetu kārtējam gadam	Vismaz divreiz gadā Latvijas speciālistu dalība

[13] Ja ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[13]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
	politikas veidotāju konsultācijās, NATO un ES drošības, aizsardzības un militārās sadarbības iniciatīvās un platformās			NBS, MilCERT	paredzētie finanšu līdzekļi.	starptautiskajās kiberdrošības mācībās
4.3.	Turpināt esošās iniciatīvas un attīstīt starptautisko sadarbību kibernoziedzības mazināšanai. Sadarbība ar dažādām starptautiskām kibernoziedzības apkarošanas struktūrām	Pastāvīgi	IeM (VP)	ĀM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Aktīva sadarbība kibernoziedzības mazināšanā ar dažādām kibernoziedzības apkarošanas struktūrām
4.4.	Sniegt atbalstu Latvijas kiberdrošības jomas komersantiem sadarbības partneru meklējumos	Pastāvīgi	LIAA		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Sniegts atbalsts sadarbības partneru meklējumos
4.5.	Latvijas interešu formulēšana un aizstāvēšana ESAO Digitālās ekonomikas politikas komitejā un ESAO rekomendāciju digitālās politikas jomā ieviešanas koordinācija	Pastāvīgi	VARAM	AM, CERT.LV, TM, DVI, LM, SM, SPRK, CSP	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Regulāra Latvijas pārstāvja dalība komitejā. Rekomendācijas iekļautas digitālās jomas politikas plānošanas un citos dokumentos

4.5. 5. rīcības virziens "Tiesiskums kibertelpā un kibernoziedzības mazināšana"

Kibernoziegumu radītais jebkura veida kaitējums mazina uzticēšanos digitālajiem pakalpojumiem. Kibernoziedzības mazināšanai nepieciešama rīcība divos pamatvirzienos – preventīvs darbs noziedzīgu darbību īstenošanas mazināšanai un efektīva noziedzības apkarošana (5.1. un 5.2. uzdevums). Vienlaikus jāuzsver arī sabiedrības līdzdalības aspekts, kas balstās sabiedrības izpratnē par kiberdrošību, jo plašāka sabiedrības izpratne par kiberdrošības riskiem palīdz novērst kibernoziegumus. Tā tiek panākta, aplūkojot kibernoziedzības problemātiku dažādos formātos (izglītības iestādes, pētnieciskie centri, konferences u. c.) un informējot cilvēkus, balstoties uz drošas uzvedības pētījumiem un analīzi.

Kibernoziedzības apkarošanu varētu atvieglot, uzlabojot tiesībsargājošo iestāžu tehniskās iespējas identificēt interneta protokola adreses, no kurām veikta piekļuve noteiktiem e-pakalpojumiem vai informācijas resursiem. Šobrīd elektronisko sakaru komersanti IPv4 adrešu trūkuma dēļ aktīvi izmanto tīkla adrešu translēšanu. Latvijā vienu IPv4 adresi izmanto līdz pat 100 lietotāji – tas rada dažādas problēmas, tai skaitā drošības jomā, jo tiesībsargājošās iestādes no saglabājamajiem datiem ar grūtībām spēj identificēt galalietotāju, kurš veicis

pretlikumīgas darbības. Risinājums šai problēmai ir uzsākt IPv6 ieviešanu valsts pārvaldē, tādējādi veicinot interesi par IPv6 ieviešanu arī privātajā sektorā (5.3. uzdevums).

5. tabula

5. rīcības virziena "Tiesiskums kibertelpā un kibernoziedzības mazināšana" uzdevumi

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[14]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
5.1.	Attīstīt Valsts policijas un valsts drošības iestāžu spējas izmeklēt kiberdrošības incidentus, stiprināt Valsts policijas un valsts drošības iestāžu darbībspēju	Pastāvīgi	IeM (VP), TM, AM		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Palielinātas Valsts policijas un valsts drošības iestāžu spējas, tai skaitā ekspertīze, izmeklējot noziedzīgus nodarījumus pret IKT, īstenojot valsts iekšējās drošības uzraudzību un uzraugot kritisko infrastruktūru
5.2.	Valsts policijas darbinieku, tiesnešu, prokuroru apmācības īstenošana, turpinot Tiesu administrācijas un Eiropas Sociālā fonda projektā "Justīcija attīstībai" organizētās starpdisciplinārās sadarbības mācības[15]	Pastāvīgi	TM, IeM (VP)		Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi.	Īstenots Valsts policijas darbinieku, tiesnešu un prokuroru apmācības plāns
5.3.	Palielināt interneta lietotāju identificēšanu, veicinot pāreju uz IPv6 valsts pārvaldē, tādējādi motivējot privāto sektoru sekot paraugam	2020. g. 4. cet.	SM	VARAM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. Pašvaldības un pašvaldību iestādes uzdevumu	Uzlabota iespēja tiesībsargājošām iestādēm identificēt e-pakalpojuma vai informācijas resursa lietotājus

[14] Ja ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

[15] Mācības ir turpinājums ES struktūrfondu un Kohēzijas fonda 2014.–2020. gada plānošanas perioda darbības programmas "Izaugsme un nodarbinātība" 3.4.1. specifiskā atbalsta mērķa "Paaugstināt tiesu un tiesībsargājošo institūciju personāla kompetenci komercdarbības vides uzlabošanas sekmēšanai" projekta Nr. 3.4.1.0/16/I/001 "Justīcija attīstībai" ietvaros notikušajām mācībām.

Nr.	Uzdevums	Izpildes termiņš	Atbildīgā institūcija[14]	Iesaistītās institūcijas	Nepieciešamais finansējums (indikatīvi) un tā avoti	Sasniedzamais rezultāts un rezultatīvais rādītājs (ja iespējams)
					realizē, ja iespējams, plānojot uzdevuma realizācijai nepieciešamos finanšu līdzekļus pašvaldību un pašvaldību iestāžu budžetu izstrādes laikā, vienlaikus ievērojot Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" prasības.	

5. 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. 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 noteikto uzdevumu izpildei nepieciešamais finansējums un tā iespējamie avoti ir norādīti Stratēģijas 4. nodaļā un pielikumā (informācija dienesta vajadzībām).

Ja Stratēģijas 4. nodaļas 1.–5. tabulā un pielikuma (informācija dienesta vajadzībām) 1. un 2. tabulas ailē "Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, institūcijas savstarpēji vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā finansējuma pieprasīšanu, tādēļ finansējuma sadale starp institūcijām ir indikatīva.

Stratēģijā paredzēto uzdevumu īstenošana 2019. gadā tiks nodrošināta Stratēģijā minētajām atbildīgām institūcijām piešķirto valsts budžeta līdzekļu ietvaros, savukārt jautājums par papildu valsts budžeta līdzekļu piešķiršanu 2020.–2022. 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.

6. tabula

Kopsavilkums par Stratēģijā iekļauto rīcības virzienu īstenošanai nepieciešamo indikatīvo finansējumu pa gadiem (EUR)

Rīcības virziens	2019. gads	2020. gads	2021. gads	2022. gads	Kopā
1. Kiberdrošības veicināšana, digitālās drošības risku mazināšana	0	0	0	0	**0**
2. IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana	0	13061560	9332985	7382169	**29776714**
3. Sabiedrības izpratne, izglītība un pētniecība	0	0	0	0	**0**
4. Starptautiskā sadarbība	0	0	0	0	**0**
5. Tiesiskums kibertelpā un kibernoziedzības mazināšana	0	0	0	0	**0**
Kopā	**0**	**13061560**	**9332985**	**7382169**	**29776714**

7. 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.:	0	-13061560	-9332985
Izmaiņas valsts budžeta izdevumos	0	-13061560	-9332985
Izmaiņas pašvaldību budžeta izdevumos	0	*	*
Kopējā finansiālā ietekme:	0	-13061560	-9332985
Finansiālā ietekme uz valsts budžetu	0	-13061560	-9332985
Finansiālā ietekme uz pašvaldību budžetu	0	*	*
Detalizēts ieņēmumu un izdevumu aprēķins (ja nepieciešams, detalizētu ieņēmumu un izdevumu aprēķinu pievieno politikas plānošanas dokumenta pielikumā. Ietekmi uz valsts un pašvaldību budžetiem atsevišķi norāda valsts un pašvaldību budžetam)	Atbildīgās institūcijas Stratēģijā paredzētos uzdevumus 2019. gadā īstenos piešķirto valsts budžeta līdzekļu ietvaros. Jautājums par papildu valsts budžeta līdzekļu piešķiršanu 2020.–2022. 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.		

	Detalizēti aprēķini par papildu nepieciešamo valsts budžeta finansējumu ir norādīti Stratēģijas pielikumā (informācija dienesta vajadzībām).		
Izmaiņas budžeta izdevumos 2022. gadā	2022. gadā -7382169	-	-

* Atsevišķu Stratēģijā paredzēto uzdevumu īstenošana ietekmēs pašvaldību budžetu. Izmaiņas pašvaldību budžeta izdevumos un finansiālo ietekmi uz pašvaldību budžetu šobrīd nav iespējams aprēķināt dēļ kiberdrošības vides un ietekmēto pašvaldību skaita mainības, kā arī finansiālā ietekme būs atkarīga no veida, kādā atbildīgās institūcijas realizēs tām uzdotos uzdevumus. Atbildīgās institūcijās, plānojot un realizējot Stratēģijā paredzētos uzdevumus, izvērtēs to ietekmi un sagatavos aprēķinus par finansiālo ietekmi uz pašvaldību budžetu.

6. Pārskatu iesniegšanas kārtība

Aizsardzības ministrija sadarbībā ar visām iesaistītajām institūcijām un NITDP līdz 2022. gada 1. maijam iesniedz Ministru kabinetā informatīvo ziņojumu par Stratēģijas uzdevumu īstenošanas novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem.

7. 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.

Ministru prezidenta biedrs, aizsardzības ministrs Artis Pabriks