Pamatnostādnes „Latvijas kiberdrošības stratēģija 2014.–2018.gadam”

SATURS

1. Ievads

Latvijā ir izveidojusiesinformācijas sabiedrība, kurāvalsts pārvalde, sabiedrība un ekonomika ir atkarīga no informācijas un komunikāciju tehnoloģiju (IKT) sniegtajām iespējāmun pakalpojumiem. Latvijas ilgtspējīgas attīstības stratēģija paredz veicināt tālāku modernas un inovatīvas sabiedrības izveidi, atvērtu jaunām idejām un augstu tehnoloģiju izmantošanai, kas kalpotu par pamatkapitālu Latvijas ekonomikas izaugsmei un konkurētspējai pasaulē.[1]

Līdz ar pieaugošoIKT izmantošanu sabiedrībā, valsts pārvaldē un ekonomikā to nelikumīga izmantošana, bojāšana, paralizēšana vai iznīcināšana var radīt draudus valsts un sabiedrības drošībai, sabiedriskajai kārtībai un ekonomiskajai darbībai, kā arī kavēt tālāku valsts ekonomikas izaugsmi. Mērķtiecīgi vai neapzināti rīkojoties, ar IKT palīdzību iespējams traucēt vai apturēt valsts informācijas sistēmu un elektronisko sakaru tīklu darbību, kā arī apgrūtināt valsts politisko, ekonomisko un militāro lēmumu pieņemšanas mehānismu funkcionēšanu, radīt finansiālus zaudējumus, dezinformēt sabiedrību un izraisīt tehnogēnas avārijas. Nedrošība kibertelpā var ietekmēt uzticamību IKT lietošanai un attiecīgi kavēt modernas un inovatīvas sabiedrības attīstību.Politiski, sabiedriski vai ekonomiski jūtīgu notikumu attīstības situācijā pret Latviju var tikt vērsti liela apmēra elektroniskie uzbrukumi. Droša un uzticama informācijas sabiedrība un e-pārvalde valstī nav iespējama bez nacionālas kompetences kiberdrošībā un kriptogrāfijā.

Ņemot vērā līdzšinējās tendences,kur pieaug sabiedrības līdzdalība kibertelpā,IKT pakalpojumu klāsts un izmantošana, attiecīgi pieaugelektronisko uzbrukumu skaits un metodes, ar kādām tie veikti.[2]

Lai mazinātu un novērstu riskus un apdraudējumus kibertelpā, nepieciešama vienota un koordinēta Latvijas kiberdrošības politika, kas aptver visas iesaistītās nozares, valsts un privāto sektoru. Pamatnostādnes „Latvijas kiberdrošības stratēģija" nosaka stratēģiskās prioritātes kiberdrošības politikas veidošanā, un tālākā darba organizēšanai tiek izstrādāts atbilstošs rīcības plāns. Pamatnostādnes izstrādātas kopskatā ar starptautisko organizāciju, jo īpaši ES un NATO, dokumentiem kiberdrošības jomā, kā arī saskaņā ar Nacionālās drošības koncepcijā un Valsts aizsardzības koncepcijā noteiktajiem pasākumiem.

2. Politikas mērķi un pamatprincipi

Kiberdrošības politikas mērķis ir drošaun uzticamakibertelpa, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana.

Īstenojot kiberdrošības politiku, tiek ievēroti šādi pamatprincipi - attīstība, sadarbība, atbildība un atvērtība.

Attīstība – tikai pastāvīgi un sistemātiski attīstot un pilnveidojotprasmes IKT nozarēun tās drošības specializācijā, var efektīvi aizsargāties pret strauji pieaugošiem draudiem kibertelpā.

[1] Latvijas ilgtspējas attīstības stratēģija līdz 2030.gadam.
[2] *Symantec* 2013.gada Interneta drošības draudu ziņojums par uzbrukumu un ievainojamības pieaugumu pasaulē.

Sadarbība – tikai sadarbojoties gan nacionālā, gan starptautiskā mērogā, iespējams efektīvi aizsargāties pret draudiem kibertelpā, kuru neierobežo valstu ģeogrāfiskās un institūciju administratīvās robežas.

Atbildība – tikai tad, ja visaskibertelpā iesaistītās puses, tajā skaitā indivīdi, valsts institūcijas, komersanti, ir informēti un apzinās atbildību par savas darbības vai bezdarbības ietekmi uz savu un citu drošību, ir iespējams efektīvi samazināt riskus kibertelpā.

Atvērtība – kiberdrošības politika īstenojama, veicinot pēc iespējas plašāku informācijas un komunikāciju tehnoloģiju pieejamību, respektējot indivīda tiesības un pamatbrīvības, meklējot līdzsvaru starp brīvību, privātumu un drošību, kā arī veicinot labo praksi, ētiku un standartus kibertelpā.

3. Latvijas kiberdrošības situācijas raksturojums

Mūsdienu sabiedrībaIKT izmanto arvien plašāk,gan tiešā veidā iegūstot informāciju un to apstrādājot, gan rodot jaunus un plašai auditorijai pieejamus pašizpausmes veidus, izmantojot ērtus un daudzveidīgus savstarpējās saziņas rīkus un platformas un saņemot pakalpojumus. Kopumā 75,8 % Latvijas iedzīvotāju ir lietojuši internetu, bet 70,3 % iedzīvotāju internetu lieto vismaz reizi nedēļā[3], lielākajās Latvijas bankās elektronisko transakciju skaits ir lielāksnekā 90 % no kopējā transakciju skaita,[4]un vairāk nekā 25 % valsts institūciju pakalpojumu pieejami elektroniski[5].

PlašaIKT izmantošana ir izmainījusisabiedrības ikdienas paradumus, un ir izveidojusiesvirtuālā vide, kur saplūst fiziskā un digitālā rīcība. Priekšstatu, ka IKT ir tikai šauras profesionāļu grupas interešu sfērā, pakāpeniski aizstāj izpratne, ka ar IKT lielākā vai mazākā mērā ir saistīta visa sabiedrība, un tuvākajos gados IKT nodrošinātu un atbalstītu pakalpojumu klāsts Latvijā palielināsies. Tā kā IKT tiek plašiizmantotas, visiem sabiedrības dalībniekiem – no IKT lietotājiem līdz vadītājiem, lēmuma pieņēmējiem un likumdevējiem – ir jābūt izpratnei par kibertelpas darbības un drošības pamatprincipiem.

IKT risinājumiem un pakalpojumiem ir komplicēta uzbūve, bet plaša pieejamība, tāpēc kibertelpa ir viegli izmantojama, lai nodarītu kaitējumu indivīdam, sabiedrības grupai vai valstij kopumā. Tāpat, izmantojot IKT rīkus, var ierobežot indivīda tiesības un pamatbrīvības vai pārkāpt tiesības uz privātumu un personu datu aizsardzību.

Situāciju Latvijas kibertelpā ik dienas raksturo ievērojams skaits IKT drošības incidentu, sākot ar vairākiem augstas nozīmības incidentiem līdz simtiem zemas nozīmības incidentu, kas vienlīdz skar gan valsts un pašvaldību institūcijas, gan komersantus un fiziskas personas. Saskaņā ar CERT.LV pārskatu 2012.gadā identificēti 4794 augstas prioritātes incidenti un vairāk nekā 200 tūkstoši zemas prioritātes incidentu.[6]Attīstās tendence, ka politiski, sabiedriski vai ekonomiski jūtīgus notikumus pavada mērķtiecīgi organizēti uzbrukumi kibertelpā. Īpaši paaugstināta riska situācija Latvijā būs 2015.gadā, nodrošinot prezidentūru ES Padomē.

---

[3] Centrālās statistikas pārvalde. Iedzīvotāji, kuri lieto datoru / internetu gada sākumā. 2012.
[4] Latvijas Interneta asociācija. Latvijas internetbanku pētījums. 2011.
[5] Vides aizsardzības un reģionālās attīstības ministrija. Visu valsts īstenoto publisko pakalpojumu izvērtēšanas un klasifikācijas rezultāti. Kopsavilkums par visu resoru pakalpojumiem. Versija 1.0.2012.
[6]CERT.LV 2012.gada pārskats.

Lai mazinātu gadījumus, kad sabiedrībai tiek nodarīts kaitējums, izmantojot IKT, ir būtiski izstrādāt visaptverošu pasākumu kopumu, kas aizsargātu kibertelpu un tās pakalpojumus. Tā īstenošanai stratēģijā ir izvirzīti pieci prioritāri rīcības virzieni:

1. Kiberdrošības pārvaldība un resursi.
2. Tiesiskums kibertelpā un kibernoziedzības mazināšana.
3. Sabiedrības izpratne, izglītība un pētniecība.
4. Gatavība un rīcībspēja krīzes situācijās.
5. Starptautiskā sadarbība.

4. Rīcībasvirzieni

4.1. Kiberdrošības pārvaldība un resursi

IKT risinājumi un pakalpojumi valstī tiek veidoti, attīstīti un uzturēti kā publiskajā, tā privātajā sektorā. Lai piedāvātie risinājumi un pakalpojumi būtu uzticami, droši un nepārtraukti, nepieciešams piemērot informācijas drošības prasības, standartus un labo praksi visā to dzīvesciklā, ietverot risku analīzē balstītu drošības plānošanu, novērtējot politiskos, ekonomiskos, sociālos, personas datu aizsardzības un tiesiskos aspektus.Latvijas kiberdrošības īstenošanā iriesaistīts plašs, daudzveidīgs ieinteresēto pušu loks,tāpēc nepieciešams izveidot efektīvu kiberdrošības pārvaldības modeli.

Nacionālā kiberdrošība

Nacionālākiberdrošība jāaplūko trīs dimensijās – infrastruktūra, pakalpojumi un procesi –, kuros nepieciešams nodrošināt informācijas drošību.Šobrīd kiberdrošības pārvaldība tiek organizēta daļēji centralizētā modelī, kurā vadošās iestādes (atbilstoši noteiktajai kompetencei) veic kiberdrošības stratēģijas, metodoloģijas un koordinācijas funkciju, savukārt konkrēto IKT risinājumu un pakalpojumi pārziņi patstāvīgi nodrošina noteikto prasību praktisku ieviešanu un izpildi. Nacionālās kiberdrošības pārvaldības pamatā ir savstarpējā sadarbība, kur katra valstsiestāde pilda savas funkcijas, tajā skaitā kibertelpā, un sadarbojas ar pārējām iesaistītajām pusēm tieši vai ar Nacionālās informācijas tehnoloģiju drošības padomes (turpmāk – Padome) starpniecību. Padome ir izveidota,pamatojoties uz Informācijas tehnoloģiju drošības likumu, kas nosaka kiberdrošības politikas veidošanu nacionālajā līmenī un uzdod Padomei koordinēt kiberdrošības politikas izstrādi, uzdevumu un pasākumu plānošanu un veikšanu. Padome ir centrālā nacionālā institūcija valsts un privātā sektora informācijas apmaiņai un sadarbībai, un tās darbību nodrošina Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļa.

Nacionālo kiberdrošības politiku veido (shēma Pielikumā Nr.1):

1. **Aizsardzības ministrija (AM)**koordinē informācijas tehnoloģiju drošības un aizsardzības politikas veidošanu un īstenošanu, kā arī līdzdarbojas starptautiskās sadarbības nodrošināšanā. AMNacionālās kiberdrošības politikas koordinācijas nodaļa organizē un sniedz atbalstu kiberdrošības politikas īstenošanai.
2. **Ārlietu ministrija (ĀM)** koordinē starptautisko sadarbību un Latvijas dalību dažādās ar kiberdrošību saistītās starptautiskās iniciatīvās.
3. **Finanšu un kapitāla tirgus komisija (FKTK)** regulē un pārrauga finanšu un kapitāla tirgus dalībnieku darbību kibertelpā, **Latvijas Banka (LB)** veicina maksājumu sistēmu drošu un raitu darbību, un**kredītiestādes** atbild par savas nozares elektronisko pakalpojumu drošu pieejamību.

4. **Ekonomikas ministrija (EM**) izstrādā ekonomikas politiku un veicina konkurētspējasun inovāciju attīstību.
5. **Iekšlietu ministrija (IeM)**,**Valsts policija (VP)** un **Drošības policija (DP)**īsteno noziedzības apkarošanas, sabiedriskās kārtības un drošības aizsardzības, personas tiesību un likumīgo interešu aizsardzības politiku, kā arī koordinē krīzes situāciju risināšanu.
6. **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.
7. **Izglītības un zinātnes ministrija (IZM)** veicina sabiedrības zināšanas un izpratni par kibertelpu un drošutās lietošanu.
8. **Labklājības ministrija (LM)** īsteno sociālās un bērnu tiesību aizsardzības politiku.
9. **Latvijas Drošāka interneta centra *Net-SafeLatvia***darbību nodrošina Latvijas Interneta asociācija, un tas izglīto sabiedrību par iespējamajiem riskiem un apdraudējumiem interneta vidē un veicina drošu interneta satura lietošanu.
10. **Nacionālie bruņotie spēki (NBS)** un **Kiberaizsardzības vienība(KAV)**sniedz atbalstu krīzes situācijās.
11. **Nozares nevalstiskās organizācijas** sniedz atbalstu, konsultē un sadarbojas ar Padomi kiberdrošības politikas veidošanā un īstenošanā[7].
12. **Satiksmes ministrija (SM)** organizē sakaru politikas īstenošanu.
13. **Satversmes aizsardzības birojs (SAB)** uzrauga kritisko infrastruktūru.
14. **Tieslietu ministrija (TM)**un **Datu valsts inspekcija (DVI)**izstrādā, organizē un koordinē tiesību politiku personas datu aizsardzības, informācijas atklātības un elektronisko dokumentu uzraudzības jomā.
15. Valsts akciju sabiedrība **„Latvijas Valsts radio un televīzijas centrs" (LVRTC)**ir vienīgais uzticamu sertifikācijas pakalpojumu sniedzējs, kurš nodrošina elektronisko identifikācijas karšu un elektroniskā paraksta infrastruktūru.
16. **Vides aizsardzības un reģionālās attīstības ministrija (VARAM)**organizē valsts IKT pārvaldību un koordinē publisko pakalpojumu elektronizāciju, bet **Valsts reģionālās attīstības aģentūra (VRAA)** nodrošina valsts IKT koplietošanas risinājumu darbību un attīstību.

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. Incidentu gadījumos valsts un pašvaldību institūcijām un kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem ir paredzēta noteikta rīcība.

Privātajā sektorā informācijas drošības pārvaldība balstās uz komercdarbības ilgtspēju un drošu un uzticamu pakalpojumu sniegšanu. Atsevišķās nozarēs ir regulējoši normatīvie akti, kas, piemēram, attiecas uz kredītiestādēm, elektroniskajiem pakalpojumu sniedzējiem unfizisko personu datu aizsardzību, taču labā prakse un standarti IKT risinājumu drošībā nav plaši izmantoti. Latvijas elektronisko sakaru komersantu tirgus ir sadrumstalots, un daļa no

[7]Padomes esoši sadarbības partneri: biedrība „ISACA Latvijas nodaļa", Latvijas Atvērto tehnoloģiju asociācija, Latvijas Informācijas un komunikācijas tehnoloģijas asociācija, Latvijas Interneta asociācija, Latvijas Komercbanku asociācija, Latvijas Tirdzniecības un rūpniecības kamera.

pakalpojumu sniedzējiem nepilda tiesību aktos noteiktās prasības, radot drošības riskus gan klientiem, gan citiem IKT infrastruktūras lietotājiem ne tikai Latvijā, bet arī ārvalstīs.

Saskaņā ar IT drošības likumu ir izveidota nacionālā Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV, kas uztur vienotu kibertelpā notiekošo darbību atainojumu, kā arī sniedz atbalstu Latvijas un ārvalstu valsts un pašvaldību institūcijām, komersantiem un fiziskām personām IT drošības incidentu novēršanā vai koordinē drošības incidentu novēršanu. Pieaugot aktivitātei kibertelpā, CERT.LV sadarbībā ar valsts un privātā sektora iestādēm jāattīsta resursi, kas ļautu apkopot tehnisko informāciju par incidentiem kibertelpā, to uzglabāt un arhivēt analīzei un izvērtēšanai.

Nepieciešamā rīcība:

1. Sadarbojoties valsts, nevalstiskā un privātā sektora pārstāvjiem, nostiprināt koordinētu nacionālās politikas kiberdrošības jautājumos veidošanu, īstenošanu un izvērtēšanu Nacionālās IT drošības padomes ietvaros.Aizsardzības ministrijai nostiprināt vadošo lomu kiberdrošības politikas koordinētā izstrādē un īstenošanā.
2. Izveidot informācijas apmaiņas vidi (platformu), veicinot informācijas apmaiņu uzņēmēju vidū par aktuālajiem kiberdrošības apdraudējumiem, problēmām, risinājumiem, labo praksi un tās piemērošanu.
3. Veikt nacionālās kiberdrošības risku izvērtējumu.
4. Veicināt labas drošības pārvaldības standartus un praksi valsts un privātajā sektorā, veidojot izpratni par IKT drošību uzņēmējdarbības vidē un organizējot vadošo darbinieku regulāru apmācību.
5. Pilnveidotelektronisko sakaru komersantu drošības prasību īstenošanas un uzraudzības mehānismu.
6. Pilnveidot CERT.LV spējasnovērot, analizēt un novērst IT drošības incidentus un sadarboties ar NATO un ES partneriem informācijās apmaiņā.
7. Attīstīt CERT.LV resursus un kompetences veikt centralizētus drošības testus.

Valsts IKT pārvaldība

Kiberdrošība nacionālajā līmenī ir cieši saistīta ar valsts IKT pārvaldības sistēmu, kuru šobrīd daļēji nosaka Valsts informācijas sistēmu likums. Tās tālākā attīstība ir iezīmēta valsts IKT pārvaldības organizatoriskā modeļa koncepcijā. Koncepcija paredz daudzus uzdevumus valsts IKT optimizācijai un valsts IKT pārvaldības procesu pilnveidei, kas valsts pārvaldei ļautu nonākt pie homogēnākas, koplietojamākas, profesionālāk un racionālāk uzturētas valsts IKT infrastruktūras, kuras ekspluatācijā būtu iespējams piesaistīt labāk motivētu personāla resursu ar augstāku specializācijas pakāpi un augstākām profesionālajām kompetencēm, tādējādi paaugstinot arī kopējo valsts IKT drošības līmeni. Cita starpā valsts IKT optimizācija perspektīvā ļautu koncentrēt resursus valsts IKT risinājumu drošības pilnveidei arī no tehnoloģiskā aspekta, piemēram, veidojot koplietojamus darbības nepārtrauktības risinājumus, u.c. Attiecībā uz valsts IKT drošības pārvaldību koncepcija paredz izstrādāt un ieviest standartus un vadlīnijas elektronizēto valsts pārvaldes procesu darbības nepārtrauktībai, uzticamībai un drošībai.

Izmantotie valsts IKT risinājumi un īpaši valsts informācijas sistēmas (VIS) satur tādu informāciju, kuras nelikumīga izpaušana vai iegūšana, sagrozīšana vai dzēšana var radīt būtisku kaitējumu konkrētai personai, sabiedrībai vai valsts interesēm. Liedzot piekļuvi VIS vai traucējot atbalsta sistēmu darbību, var tik daļēji vai pilnībā paralizēts publiskās pārvaldes darbs.Līdz ar to ir svarīgi, lai valsts IKT risinājumu izstrāde, ieviešana un ekspluatācija, tajā

skaitā drošības pārvaldība, tiktu īstenota racionāli, efektīvi, pārskatāmiun savstarpēji saskaņoti, ievērojot nozares labākās prakses pieredzi un vadlīnijas, pēc iespējas mazinot IKT drošības apdraudējumu rašanos kā kļūdas, tā arī apzinātas rīcības dēļ.

Valsts informācijas sistēmu likums nosaka vienotu tehnisko un organizatorisko prasību līmeni visām reģistrētām sistēmām neatkarīgi no tās funkcionalitātes, uzkrātās informācijas vērtības un ietekmes uz publiskās pārvaldes funkciju izpildi kā pašā iestādē, tā arī ārpus tās. Prasību diferencēšanas trūkums rada neatbilstošu slogu dažādas nozīmes un apjoma sistēmām, kā arī vēlmi izvairīties no sistēmas reģistrācijas. Prasību diferenciācija un sistēmu grupēšana ļautu precīzāk piemērot atbilstošu tiesisko regulējumu noziedzīga nodarījuma gadījumā.

VARAM veiktā situācijas analīze liecina, ka puse valsts informācijas sistēmu pārziņu nenodrošina drošības pārvaldības pasākumus, jo nav motivēti vai kompetenti. Valsts IKT drošības uzraudzības un kontroles sistēma ir nepietiekama.

Nepieciešamā rīcība

1. Turpināt valsts IKT pārvaldības organizatoriskā modeļa koncepcijā noteikto pārvaldības uzlabošanas pasākumu īstenošanu, kas paredz vienotas valsts IKT arhitektūras izstrādi, pārvaldības procesu, standartu un vadlīniju izstrādi vai pilnveidi.
2. Izstrādāt normatīvo regulējumu vienotai valsts IKT nodrošinājuma pārvaldībai, paredzot risku analīzē balstītu dažādu informācijas sistēmu grupēšanu un attiecīgi diferencētu drošības pārvaldības prasību ietvaru.
3. Pilnveidot valsts IKT risinājumu un infrastruktūras turētāju izpratni un zināšanas, īstenojot apmācību programmas valsts pārvaldes iestāžu vadības līmeņa personālam un IKT drošības pārvaldībā iesaistītajam personālam.
4. Izvērtēt valsts IKT drošības pārvaldības uzraudzības efektivitāti, atbildību un soda sankcijas par drošības pārvaldības pasākumu neīstenošanu, kā arī noteikt minimālās prasības drošības pārvaldnieku darbam.
5. Organizēt neatkarīgas iestādes veiktas valsts IKT risinājumu un infrastruktūras ārpuskārtas pārbaudes un drošības testus.
6. Izstrādāt kārtību, kādā iestādes regulāri atskaitās vienotai kompetentai institūcijai par informācijas drošības pasākumu realizāciju.
7. Pašvaldību IKT resursu drošības pārvaldības uzlabošanai attīstīt sadarbību Latvijas Pašvaldību savienības, pašvaldību un valsts institūciju starpā.

Kritiskā infrastruktūra

Valstij un sabiedrībai būtisku pamatfunkciju veikšanai ir noteikta informācijas tehnoloģiju kritiskā infrastruktūra, lai nodrošinātu kritiskās infrastruktūras integritāti, pieejamību un konfidencialitāti.Ministru kabinets nosaka un reizi gadā pārskata to IT infrastruktūru, kuras darbības pārtraukšana var ievērojami apdraudēt valsts pastāvēšanu.[8] Informācijas tehnoloģiju kritiskā infrastruktūra ir iekļauta valsts kritiskās infrastruktūras kopumā, un sadarbībā ar drošības iestādēm un CERT.LV tās īpašnieki un tiesiskie valdītāji pastāvīgi pilnveido drošības pasākumus. Kritiskās infrastruktūras drošības pasākumu plānošanu un īstenošanu nosaka Ministru kabinets.[9] Zināšanu un pieredzes apmaiņai, kā arī procedūru pilnveidei kritiskās infrastruktūras pārstāvji tiek regulāri iesaistīti CERT.LV rīkotās

[8] 2010.gada 1.jūnija Ministru kabineta noteikumi Nr.496 „Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība".

[9]2011.gada 1.februāra Ministru kabineta noteikumi Nr.100 „Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība".

mācībās.

Nepieciešamā rīcība:

1. Uzlabot informācijas un pieredzes apmaiņu par incidentiem, kritiskās infrastruktūras aizsardzību un risku novēršanu starp kritiskās infrastruktūrām turētājiem, CERT.LV un valsts drošības iestādēm.
2. Organizēt kopīgas krīzes mācības un ielaušanās pārbaudes nacionālā, reģionālā un starptautiskā līmenī un sadarbojoties ar Nacionālo bruņoto spēku (NBS) Kiberaizsardzības vienību.
3. Stiprināt valsts kritisko IKT resursu drošību, attīstot tehniskos rīkus automatizētai drošības nodrošināšanai un kontrolei, kā arī uzlabot drošības personāla kapacitāti, zināšanas un savstarpējo sadarbību.

Cilvēkresursi

Situāciju valsts un pašvaldību institūcijās raksturo būtiski atšķirīgie cilvēkresursi un materiālie resursi, sākot no institūcijām ar labi apmaksātiem augstas kvalifikācijas darbiniekiem un moderniemtehniskajiem resursiem un beidzot ar – vairākumā gadījumu – institūcijām ar nepietiekamas kvalifikācijas darbiniekiem un zemas kvalitātes informācijas tehnoloģijām. Tas veido atšķirīgu tiesību aktos noteikto pienākumu izpildes līmeni informācijas drošības pārvaldības jomā valsts pārvaldē. Vienlaicīgi ierobežotais augsta līmeņa speciālistu piedāvājums darba tirgū nenodrošina privātā sektora pieprasījumu, un kompānijas izmanto ārpakalpojumus funkciju īstenošanai.

Latvijas darba tirgū IKT drošības pārvaldības un drošības tehnoloģiju speciālistu skaits ir neliels. Nav noteikts IKT drošības pārvaldnieka profesijas standarts un sertifikācija šādai darba specialitātei, un studiju programmas datorikā, datorzinātnē un informācijas tehnoloģijās mērķtiecīgi nesagatavo ekspertus šajā specializācijā. IKT drošības pārvaldniekam valsts pārvaldes iestādēs ir noteiktas minimālas kompetences prasības. Valsts un pašvaldību institūciju IT speciālisti piedalās apmācības semināros „Esi drošs" un ikgadējās instruktāžās institūcijās, taču apgūtais zināšanu apjoms ir ierobežots un tā izmantošana praksē netiek trenēta un pārbaudīta.

Nepieciešamā rīcība:

1. Izvērtēt un aktualizēt esošo ar IKT saistīto profesiju standartu prasības, iekļaujot tajos prasības pēc kiberdrošības zināšanām un prasmēm.
2. Definēt, paaugstināt un izvērtēt par kiberdrošību atbildīgo speciālistu profesionālās kompetences un veicināt ārvalstīs iegūto kiberdrošības speciālistu sertifikātu izmantošanu kompetences apliecināšanai.
3. Veicināt augstākās izglītības iestāžu ieguldījumu kiberdrošībā, iekļaujot kiberdrošības specializācijas elementus mācību programmās.
4. Veikt darba tirgus dinamikas analīzi par kiberdrošības speciālistu pieprasījumu, piedāvājumu, atalgojumu un izglītības iestāžu sagatavoto speciālistu nodarbinātību.
5. Pilnveidot pedagogu kompetences kiberdrošības jautājumos un atbalstīt metodisko materiālu sagatavošanu.

4.2. Tiesiskums kibertelpā un kibernoziedzības mazināšana

Tiesiskas kibertelpas pamatā ir ekvivalences princips, kurš nosaka likumu un tiesisko normu ievērošanu kā fiziskajā, tā virtuālajā vidē, un valstij ir pienākums nodrošināt jebkuras

personas Satversmē paredzētās pamattiesības un brīvības un vispārīgo tiesību principu ievērošanu neatkarīgi no to piemērošanas vides. Piedāvātās tehnoloģiskās iespējas ir veicinājušas to, ka personas aizvien biežāk noziedzīgos nodarījumus veic kibertelpā. Lai veiktu šādus nodarījumus, personas izmanto automatizētu datu apstrādes sistēmu kā nozieguma izdarīšanas rīku, vēršot to pret citu aizsargātu vai publiski nepieejamu automatizētu datu apstrādes sistēmu vai tās resursiem. Automatizēta datu apstrādes sistēma var tikt izmantota arī kā medijs nelikumīgas (rasu naida kurināšana, bērnu pornogrāfijas izplatīšana u.c.) un godu un cieņu aizskarošas informācijas apritē.

Kibernoziedzības mazināšanaiir nepieciešama rīcība divos pamata virzienos – preventīvs darbs noziedzīgu darbību īstenošanas mazināšanai un efektīva noziedzības apkarošana.

Kibertelpas uzbūves un darbības komplicētība iezīmē divas problemātiskas jomas efektīvā kibernoziedzības apkarošanas īstenošanā. Pirmkārt, izpratne par jēdzienu „būtisks kaitējums" un tā piemērošanu ir svarīgs priekšnosacījums noziedzīga nodarījuma sastāva konstatācijai un pareizai noziedzīga nodarījuma kvalifikācijai un sodāmībai. Otrkārt, izmeklēšanas veikšana un pierādījumu apkopošana kibertelpā prasa specifiskas zināšanas.

Preventīva darba īstenošanai svarīga ir sakārtota IKT un tās drošību regulējošonormatīvo aktubāze un to efektīva izmantošana. Kibernoziegumu apkarošanai jāattīsta esošās spējas, nostiprinot elektroniskos pierādījumus. Izmeklēšanas veikšana, pierādījumu vākšana un izvērtēšana kibertelpā prasa specializētas zināšanas, un, lai nodrošinātu likuma spēku kibertelpā, nepieciešams pietiekams kompetences līmenis tiesībsargājošās iestādēs, prokuratūrā un tiesās.

Nepieciešamā rīcība:

1. Izvērtēt IKT nozares normatīvo aktu bāzi kā Latvijas Administratīvo pārkāpumu kodeksa un Krimināllikuma piemērošanas pamatu un pilnveidot to, lai nodrošinātu personu ar likumu aizsargāto interešu efektīvu krimināltiesisko aizsardzību kibertelpā un saistībā ar to.
2. Izvērtēt esošo situāciju un nepieciešamos grozījumus tiesību aktos, kas paredz sodāmību par kaitējumu nodarīšanu informācijas sistēmu drošībai vai darbībām, kas vērstas pret automatizētām datu apstrādes sistēmām.
3. Izstrādāt ar informācijas drošību un kiberdrošību saistīto un latviešu valodā lietoto terminoloģiju un harmonizēt tās izmantošanu tiesību aktos.
4. Izvērtēt un pilnveidot kiberdrošības jomā tiesību aktos noteikto pienākumu uzraudzību un veicināt atbalstu šo pienākumu izpildē.
5. Veicināt diskusijas un viedokļu apmaiņu par IKT jaunu noziegumu veidu identificēšanu un tiesiskās bāzes pilnveidošanu to ierobežošanai kontekstā ar starptautiskajām tendencēm.
6. Apkarot un izmeklēt kibernoziegumus, izvērtējot un pilnveidojot esošos resursus, procedūras, sadarbības mehānismus un to efektivitāti.
7. Izvērtēt un pilnveidot esošās pierādījumu iegūšanas un analīzes spējas kibernoziegumu izmeklēšanas gaitā, attīstot VP kompetenci un pilnveidojot sadarbību ar CERT.LV.
8. Izstrādāt mācību metodiskos materiālus par IKT nozari policijas darbinieku, kibernoziegumu procesu virzītāju un tiesnešu zināšanu celšanai par IKT nozari un īstenot padziļinātu apmācības programmu kibernoziegumu apkarošanas jautājumos.
9. Attīstīt vienotu noziedzīgu nodarījumu kibertelpā apkopošanas mehānismu (statistiku) policijas, prokuratūras un tiesu sistēmā.

4.3. **Sagatavotība un rīcībspēja krīzes situācijās**

Lai arī Latvijā ir izveidotas institūcijas, kas nodrošina nacionālās kiberdrošības spējas, ir izstrādāti un tiek regulāri pilnveidoti plāni rīcībai paaugstināta apdraudējuma gadījumā, izveidota sadarbība ar Iekšlietu ministriju dažādu krīzes situāciju risināšanā un sadarbībā ar privāto sektoru ir pieejama speciālistu iesaiste, esošo resursu un pasākumu kopums nav pietiekami liels un organizēts, lai efektīvi un ātri rīkotos nopietnu un plašu IKT drošības incidentu jeb kiberuzbrukumu gadījumos.

Ministru kabineta 2012.gada 7.decembra kiberkrīzes vingrinājumā tika izvērtēta esošā situācija Latvijā un apdraudējumikibertelpā, kā arī valsts rīcībā esošie resursi risku novēršanai un krīzes pārvarēšanai. Incidentu mazināšanai un krīzes novēršanai būtiska ir katras organizācijas individuāla izpratne par kiberdrošību un atbildība, kur CERT.LV var sniegt padomu ikdienas darbā vai atbalstu nopietnu un neparedzētu incidentu gadījumā.

Ņemot vērā valsts pārvaldes ierobežotos resursus un kiberkrīzes vingrinājuma secinājumus, NBStiek veidota Kiberaizsardzības vienība, kas sniegtu atbalstu CERT.LV un NBS vienībām krīzes un kara situācijās IKT drošības incidentu novēršanā un radušos seku pārvarēšanā kibertelpā, ja CERT.LV rīcībā esošie resursi nebūtupietiekami un vienības piesaiste paātrinātu neatliekamo pasākumu īstenošanu, vai ja tās rīcībā būtu speciāli resursi šo darbību veikšanai.[10] Vienība tiek veidota kā rezerves ekspertu kopums no brīvprātīgiem interesentiem valsts un privātajā sektorā atbilstoši zemessarga dienesta juridiskajai bāzei.

Lai nodrošinātu elektronisko sakaru infrastruktūras funkcionēšanu un stiprināšanu, ir jāattīsta ne tikai esošās infrastruktūras spējas (īpaši attiecībā uz tās noturību pret ārēju apstākļu iedarbību), bet arī jāveido jauna infrastruktūra valsts pamatfunkciju nodrošināšanai, it īpaši situācijās, kad ikdienā lietojamo elektronisko sakaru tīklu funkciju izpilde var būt ierobežota.

Nepieciešamā rīcība:

1. Izvērtēt krīzes situāciju definīciju, procedūras un normatīvo aktu bāzi un tāsizmantojamību iespējamas kiberkrīzes gadījumā.
2. Attīstīt NBS un Kiberaizsardzības vienības reaģēšanas spējas krīzes situācijā un plašu incidentu seku novēršanā, sasniedzot un nodrošinot vienības operacionālu rīcībspēju.
3. Attīstīt NBS informācijas tehnoloģijas un sakaru sistēmas, lai nodrošinātu NBS vadības atbalsta spējas krīzes situācijās.
4. Regulāri organizēt teorētiskas un praktiskas nacionāla mēroga mācības, tajās iesaistot arī valsts augstākās amatpersonas un komersantus, lai tādējādi attīstītu savstarpējo sapratni un koordinētu darbību krīzes situāciju pārvarēšanā.
5. Pilnveidot valsts institūciju kiberdrošības kompetenci un resursus, gatavojoties un nodrošinot Latvijas prezidējošās valsts pienākumus ES 2015.gadā, kad pret Latviju var tikt vērsti globāla rakstura elektroniskie uzbrukumi.
6. Veidot reģionālo un starptautisko sadarbību, regulāras mācības palīdzības sniegšanai un saņemšanai krīzes situācijā.
7. Izveidot ārkārtas situāciju valsts elektronisko sakaru tīklu.

[10] Aizsardzības ministrijas Nacionālo bruņoto spēku Kiberaizsardzības vienības koncepcija, Rīga, 2013.

8. Izveidot tehnoloģisko un organizatorisko risinājumu, kas valsts institūcijām nodrošina infrastruktūru ar augstu konfidencialitāti, integritāti un pieejamību valsts informācijas sistēmām.

9. Stiprināt nacionālo virtuālo ārējo elektronisko sakaru tīklu perimetru: apzināt, kategorizēt, savstarpēji koordinēt, izvērtēt riskus, veikt nepieciešamos uzlabojumus, lai nodrošinātu paļāvīgu un drošu datu plūsmu starp Latviju un citām valstīm, bet nepieciešamības gadījumā to izmantot datu plūsmu izmaiņām vai ierobežošanai starp valstīm.

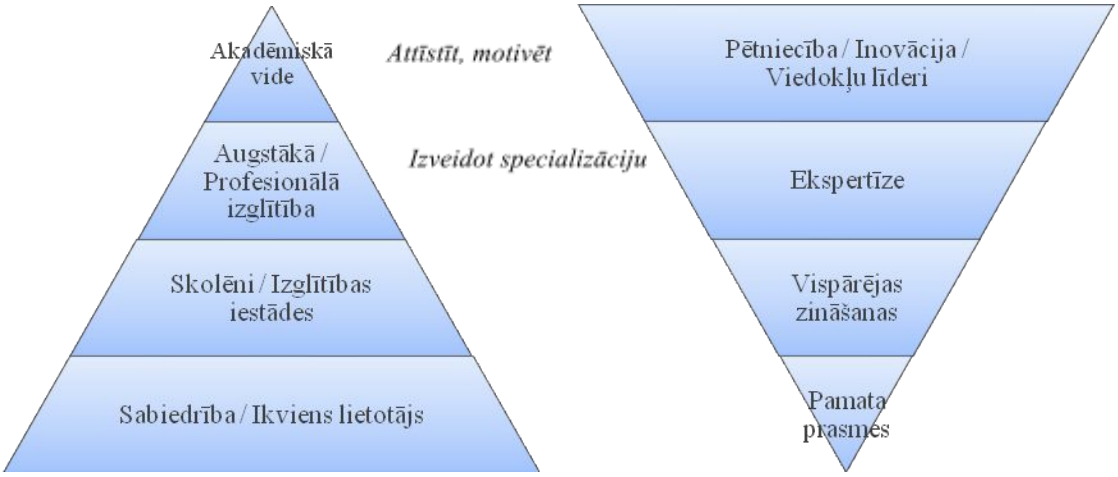
4.4. **Sabiedrības izpratne,izglītība un pētniecība**

Informēta sabiedrība ir būtiska daļa no drošas un uzticamas kibertelpas. Informētību nodrošina mērķtiecīgs un regulārs skaidrojošs darbs, ietverot valsts vadošo amatpersonu īstenoto politiku un komunikāciju, jautājumu aktualizēšanu izglītības iestādēs un regulāras ekspertu diskusijas mediju telpā.

Sabiedrības informētības līmenis par IKT apdraudējumiem, pieejamajiem rīkiem to novēršanai, savām tiesībām un to aizskārumiem elektroniskajā vidē, kā arī rīcību apdraudējuma gadījumā ir zems. Saskaņā ar CERT.LV rīcībā esošo statistiku gandrīz visos gadījumos, kad lietotāju iekārtas ir tikušas inficētas un kļuvušas par robotu tīklu sastāvdaļām (vidēji 15-20 tūkstoši mēnesī), lietotāji kaitējumu nav veikuši apzināti, bet tā cēlonis ir neatjaunināta programmatūra, antivīrusu risinājumu trūkums gadījumos, kad tiek atvērta kaitīga elektroniskā pasta pielikumi. Līdztekus sabiedrības zināšanu līmeņa celšanai nepieciešams vairāk veicināt izpratni par ētiskajām normām un morālo atbildību elektroniskajā vidē.

Lai pilnveidotu IKT lietotāju zināšanas, ir nepieciešams īstenot kompleksu pasākumu kopumu, sākot ar pamata un vidējo izglītību. Sadarbībā ar nevalstisko un privāto sektoru ir nepieciešams organizēt regulāras informatīvas kampaņas, kā arī pastāvīgu informācijas atspoguļošanu masu medijos. Šobrīd kibertelpas drošības jautājumi standartizētā veidā vispārējās izglītības satura kontekstā tiek pārbaudīti tikai informātikas eksāmenā (zināšanu testa daļā) vidējās izglītības pakāpē. Lai gan attiecīgās tematikas jautājumu vidējā izpilde ir samērā augsta (2013. – 0,79%), vispusīgi nav iespējams novērtēt izglītojamo faktisko rīcību ikdienā. Komunikāciju veids (kanāls), saturs un metodika jāpiemēro atbilstoši izvēlētajai mērķauditorijai (skat. 1. att.):

1.attēls. Kibertelpas drošības jautājumu zināšanu apjoms atbilstošajām mērķauditorijām.



Latvijā šobrīd nav akadēmisko studiju programmas un zinātniskās darbības kiberdrošības jomā, un ārvalstīs attiecīgajās jomās studējošie nav motivēti atgriezties Latvijā gan ierobežotā atalgojuma dēļ, gan arī tādēļ, ka trūkst iespēju profesionāli pilnveidoties. Saskaņā ar Pasaules ekonomikas foruma pētījumu Latvija ierindojas tikai 110.vietā pēc zinātnieku un inženieru pieejamības valstī.[11]

Lai veidotu jaunas studiju programmas, izglītotu IKT jautājumos ekspertus un citu nozaru profesionāļus (piemēram, tiesību zinātnes speciālistus), nepieciešami atbilstošas kompetences pedagogi. Kompetence jāveicina, veidojot un atbalstot drošības pētniecības grupas augstskolās un zinātniskajos institūtos. Tās piesaistītu Latvijas speciālistus, kas pašlaik strādā ārvalstīs, būtu kā pamats nacionālās kiberdrošības (t.sk. kriptogrāfijas) skolas izveidošanai, nākotnē dotu iespēju veiksmīgi piedalīties ES zinātniskos projektos un radīt komerciālus produktus ar augstu pievienoto vērtību.

Nepieciešamā rīcība:

1. Palielināt izglītības iestāžu un pedagogu kompetenci un ieguldījumu bērnu un jauniešu izglītošanā IKT kiberdrošības jautājumos, integrējot tos izglītības saturā un organizējot mācību aktivitātes, kas veido izpratni par informācijas drošību, privātuma aizsardzību un uzticamu e-pakalpojumu lietošanu, un nodrošināt iespējas bērniem un jauniešiem ziņot par pārkāpumiem internetā un saņemt psihologa atbalstu. Organizētpedagogu sistemātisku tālākizglītību kiberdrošības jautājumos.

2. Veidot ērti pieejamus un dažādām vecuma grupām diferencētus mācību un informatīvos materiālus par kiberdrošību izmantošanai izglītības iestādēs un interešu grupās.

3. Attīstīt akadēmiskās studijas un pētniecību kiberdrošības jomā, lai sagatavotu speciālistus, veicinātu inovācijas, veidotu publisko un privāto partnerību zinātnes un pētniecības atbalstam, piesaistītu Eiropas fondu, grantu un finansu instrumentus.

[11] Pasaules Ekonomikas foruma pētījums "Globālās konkurētspējas indekss 2012-2013", 227.lpp.

4. Sadarbībā ar augstskolām un zinātniskajiem institūtiem izveidot IKT drošības laboratoriju un organizēt zinātniskas konferences par kiberdrošības un kibernoziedzības aktuālajiem jautājumiem.

5. Īstenot izglītojošas un informatīvas kampaņas un citus pasākumus vispārējai sabiedrības izpratnes veicināšanai par kiberdrošību, kibernoziedzību un aktuālajiem apdraudējumiem, paplašināt dažādu IKT drošības programmatūras pieejamību.

6. Veidot informācijas un viedokļu apmaiņu starp publisko pārvaldi, nozares asociācijām, speciālistiem, ekspertiem, biznesa līderiem, kā arī sabiedriskā viedokļa veidotājiem – nevalstiskajām organizācijām un akadēmisko vidi.

7. Iesaistīties starptautiskās informatīvās iniciatīvās un platformās, izmantot ES kiberdrošības mēnesi un e-prasmju nedēļu kiberdrošības jautājumu aktualizēšanai.

8. Veicināt inovācijas kiberdrošības jomā un attīstīt kopīgu akadēmisko lieljaudas skaitļošanas (superdatora) resursu.

4.5. **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, sākot ar cilvēktiesību ievērošanu virtuālajā vidē un beidzot ar noziedzības apkarošanu, kritiskās infrastruktūras aizsardzību 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. Vienlaikus paralēli notiek daudzi savstarpēji nesaskaņoti procesi. Latvijai ir svarīgi pārzināt un iesaistīties starptautisko un reģionālo organizāciju darbā, paužot atbalstu demokrātiskas sabiedrības pamatprincipu nodrošināšanai virtuālajā vidē - tai ir jābūt ne tikai drošai, bet arī brīvai un pieejamai.

Latvija piedalās starptautiskajos procesos, tai skaitā NATO, ES, EDSO un ANO darbā, lai veicinātu drošas, brīvas un pieejamas kibertelpas nostiprināšanu. Latvija atbalsta ANO Cilvēktiesību padomes pirmo visaptverošo rezolūciju par cilvēktiesību aizsardzību virtuālajā telpā un turpinās ar savu dalību stiprināt tādas iniciatīvas kā, piemēram, Koalīcija par interneta brīvību (*FreedomOnlineCoalition)*, kas vērstas uz cilvēktiesību un pamatbrīvību, īpaši vārda brīvības, ievērošanu kibertelpā.

Latvija ir pievienojusies Eiropas Padomes konvencijai par kibernoziegumiem un tās papildu protokolam par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. Atbilstoši konvencijā paredzētajam iesaistītās valstis saskaņo savas tiesību normas, lai sadarbotos noziegumu izmeklēšanā un nodrošinātu, ka par pastrādātajiem kibernoziegumiem atbildīgie tiek saukti pie atbildības.

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 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 plānošanas dokumentiem.NATO ir pieņēmusi Kiberdrošības koncepciju un Rīcības plānu un tiem atbilstošusplānošanas dokumentus, kas nosaka nepieciešamību veicināt gan NATO kopīgo, gan katras dalībvalsts individuālo kiberaizsardzības spēju attīstīšanu.

Nepieciešamā rīcība:

1. Stiprināt sadarbību ar Baltijas un Ziemeļeiropas reģiona valstīm un pilnveidot sadarbību ar NATO, ES, EDSO un ANO, lai veicinātu IKT drošības, pieejamības un brīvības normu nostiprināšanu.
2. Atbalstīt starptautiskos centienus savstarpējas uzticēšanās un sadarbības veicināšanai, uzsverot, ka spēkā esošajām starptautiskajām tiesību normām jābūt vienlīdz piemērojamām kā fiziskajā, tā virtuālajā vidē.
3. Izveidot Baltijas valstu kopīgu studiju programmu augstskolās, lai konsolidētu reģiona izglītības resursus spēcīgu un kvalificētu speciālistu sagatavošanai.
4. Regulāri rīkot Latvijā starptautiskus pasākumus kiberdrošības jomā, iezīmējot Latviju kā valsti, kas rūpējas par IKT drošību nacionālā un starptautiskā mērogā.
5. Sagatavot un testēt 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.
6. Stiprināt kiberaizsardzības spējas, piedaloties dažādās starptautiskās mācībās, vingrinājumos, kiberuzbrukumu simulācijās gan NATO un ES, gan citos valstu sadarbības mehānismos, dodot iespēju vietējiem speciālistiem un Kiberaizsardzības vienībai pilnveidot zināšanas par jaunākajiem informācijas sistēmu drošības risinājumiem.

5. Sasaiste ar citiem attīstības plānošanas dokumentiem

Nacionālie dokumenti:

- Nacionālā drošības koncepcija
- Valsts aizsardzības koncepcija
- Informācijas tehnoloģiju drošības likums
- Valsts informācijas sistēmu likums (VARAM izstrāde)
- Latvijas ilgtspējas attīstības stratēģija līdz 2030. gadam
- Informācijas sabiedrības attīstības pamatnostādnes 2014.-2020.gadam
- Valsts informācijas un komunikācijas tehnoloģiju pārvaldības organizatoriskā modeļa koncepcija
- Elektronisko sakaru nozares politikas pamatnostādnes 2011.-2016.gadam
- Autentifikācijas likums (VARAM izstrāde)
- Aizsardzības ministrijas Nacionālo bruņoto spēku Kiberaizsardzības vienības koncepcija, 2013.gads

Starptautiskie dokumenti:

- ANO Cilvēktiesību padomes rezolūcija par cilvēktiesību aizsardzību virtuālajā telpā

- NATO Stratēģiskā koncepcija
- NATO Kiberaizsardzības koncepcija
- NATO Kiberdrošības rīcības plāns
- ES Kiberdrošības stratēģija
- Eiropas Padomes Budapeštas konvencija
- Eiropa 2020. Stratēģija gudrai, ilgtspējīgai un integrējošai izaugsmei
- ES Digitālā dienaskārtība
- Eiropas Parlamenta un Padomes Direktīva par uzbrukumiem informācijas sistēmām

6. 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 izvērtējums veidos bāzi tālākas politikas un rīcības plāna izvērtēšanā un pilnveidošanā.

Pamatojoties uz pamatnostādnēm, tiks izstrādāts plāns rīcības virzienu izpildei, kurā tiks iekļauti detalizēti darbības rezultāti un aprēķini par ietekmi uz valsts un pašvaldību budžetiem 2014. gadā un turpmākajos gados.Reizi divos gados Aizsardzības ministrija Padomes ietvaros veic pamatnostādņu un rīcības plāna īstenošanas novērtējumu un Ministru kabinetā iesniedz informatīvo ziņojumu, kā arī, ja nepieciešams, priekšlikumus pamatnostādņu aktualizācijai.

Nav tādu politikas plānošanas dokumentu, kuri būtu atzīstami par spēku zaudējušiem. Vienlaikus tiek turpināta arī Nacionālās drošības koncepcijā noteikto prioritāšu īstenošana.

7. Saīsinājumi un terminu skaidrojums

Saīsinājumi

AIM	Aizsardzības ministrija
AIP	Augstākās izglītības padome
ANO	Apvienoto Nāciju Organizācija
ĀM	Ārlietu ministrija
CCDCOE	NATO Informācijas tehnoloģiju aizsardzības izcilības centrs Tallinā
CERT.LV	Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
DP	Drošības policija
DVI	Datu valsts inspekcija
EDSO	Eiropas Drošības un sadarbības organizācija
EM	Ekonomikas ministrija
ENISA	Eiropas Tīklu un informācijas drošības aģentūra
ES	Eiropas Savienība
FKTK	Finanšu un kapitāla tirgus komisija
IeM	Iekšlietu ministrija
IEM IC	Iekšlietu ministrijas Informācijas centrs
IKT	informācijas un komunikācijas tehnoloģijas
ISACA	biedrība „ISACA Latvijas nodaļa”
IT	informācijas tehnoloģijas
IZM	Izglītības un zinātnes ministrija
NBS KAV	Nacionālo bruņoto spēku Kiberaizsardzības vienība
LB	Latvijas Banka
LDDK	Latvijas Darba devēju konfederācija
LIA	Latvijas Interneta asociācija
LIKTA	Latvijas Informācijas un komunikācijas tehnoloģijas asociācija
LKA	Latvijas Komercbanku asociācija
LM	Labklājības ministrija
LPESPS	Latvijas prezidentūras Eiropas Savienības Padomē sekretariāts
LTRK	Latvijas Tirdzniecības un rūpniecības kamera
LVRTC	Latvijas Valsts radio un televīzijas centrs
LZA TK	Latvijas Zinātņu akadēmijas Terminoloģijas komisija
MIDD	Militārās izlūkošanas un drošības dienests
NAP	Nacionālais attīstības plāns
NATO	Ziemeļatlantijas līguma organizācija
NBS	Nacionālie bruņotie spēki
NetSafe	Latvijas Drošāka interneta centra *Net-SafeLatvia*
NITDP	Nacionālā informācijas tehnoloģiju drošības padome
PMLP	Pilsonības un migrācijas lietu pārvalde
SAB	Satversmes aizsardzības birojs
SM	Satiksmes ministrija
TM	Tieslietu ministrija
VARAM	Vides aizsardzības un reģionālās attīstības ministrija
VBTAI	Valsts bērnu tiesību aizsardzības inspekcija

VIS	valsts informācijas sistēmas
VP	Valsts policija
VRAA	Valsts reģionālās attīstības aģentūra
VVC	Valsts valodas centrs

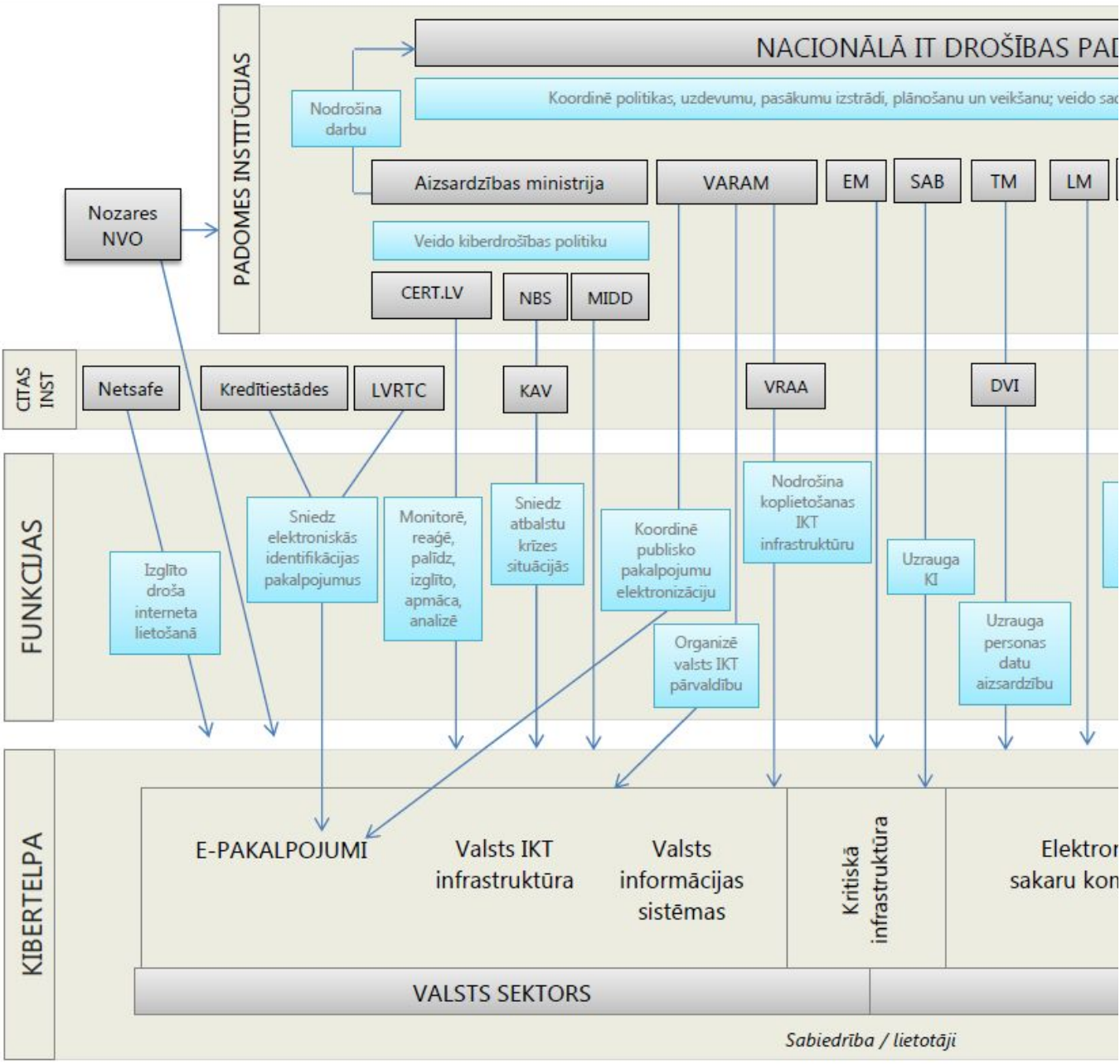
Termini

Elektronisko sakaru komersants	Komersants vai ārvalstu komersanta filiāle, kam ir tiesības veikt komercdarbību, nodrošināt publisko elektronisko sakaru tīklu vai sniegt elektronisko sakaru pakalpojumus Elektronisko sakaru likumā noteiktajā kārtībā.
Elektronisko sakaru tīkls	Pārraides sistēmas, komutācijas un maršrutēšanas iekārtas (tajā skaitā tīkla elementi, kas netiek izmantoti) un citi resursi, kas neatkarīgi no pārraidītās informācijas veida ļauj pārraidīt signālus, izmantojot vadus, radioviļņus, optiskos vai citus elektromagnētiskos līdzekļus tīklos.
E-pārvalde	Valsts un pašvaldību pārvaldes efektīva īstenošana, izmantojot informācijas un komunikāciju tehnoloģijas.
Informācijas sabiedrība	Sabiedrība, kuras locekļi prot, var un viņiem ir iespējas ar informācijas un komunikācijas tehnoloģijas palīdzību iegūt informāciju, saistīt to ar esošajām zināšanām un jauniegūtās zināšanas izmantot labklājības celšanai.
Informācijas tehnoloģijas	Tehnoloģijas, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, dzēšanu, glabāšanu, attēlošanu vai pārsūtīšanu.
Informācijas tehnoloģiju drošības incidents	Kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.
Informācijas un komunikācijas tehnoloģijas	Zināšanu, metožu, paņēmienu un tehniskā aprīkojuma kopums, kas ar datoru un sakaru līdzekļu starpniecību nodrošina jebkuras informācijas iegūšanu, glabāšanu un izplatīšanu.
Kiberdrošība	Kiberdrošība ir instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības, apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizācijas un lietotāju aktīvu aizsardzībai. Organizācija un lietotāju aktīvi ietver savienotas skaitļošanas tehnoloģijas, personālu, infrastruktūru, programmatūru, pakalpojumus, telekomunikāciju sistēmas un pārsūtītas jeb uzglabātas informācijas kopumu elektroniskajā vidē.[12]

[12]Starptautiskās telekomunikāciju savienības definīcijaangļu 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.

Pielikums Nr.1 **Nacionālās kiberdrošības politikas koordinācijas shēma**



Pielikums Nr.2

Turpmākās rīcības plānojums

- Rīcības plānojums (turpmāk – plānojums) identificē uzdevumus pamatnostādņu mērķu sasniegšanai. Plānojuma darba uzdevumi ir izstrādāti, balstoties uz pamatnostādnēs apstiprināto nepieciešamo rīcību, bet nav grupēti atbilstoši katram rīcības punktam, jo atsevišķi plāna uzdevumi vienlaikus pilda vairākus stratēģijas mērķus. Sasniedzamie politikas rezultāti ir identificēti pietiekami plaši un vispārīgi, ņemot vērā kiberdrošības komplekso dabu un straujo mainību mūsdienu vidē. Pieaugot kiberdrošības spējām un kapacitātei, palielinās incidentu, apdraudējumu un risku skaits, taču tas ne vienmēr var nozīmēt drošības līmeņa vājināšanos.

- Plānojumam ir publiskā sadaļa un sadaļa, kas ietver informāciju dienesta vajadzībām (tajā norādītie veicamie uzdevumi ir pieejami pamatnostādņu 3.pielikumā (dienesta vajadzībām)).

- Pamatnostādņu ieviešanas turpmākās rīcības plānojumā paredzētos pasākumi atbildīgās institūcijas pamatā īsteno atbilstoši piešķirtajiem valsts budžeta līdzekļiem. Atbildīgās institūcijas ir apņēmušās pildīt sev norādītos uzdevumus un, pieprasot papildu līdzekļus, izstrādās detalizētus aprēķinus, jo šobrīd 1.tabulā norādītais nepieciešamā finansējuma apmērs ir indikatīvs.

- Ja ailē „Atbildīgā institūcija" ir norādīta vairāk nekā viena institūcija, tad institūcijas savā starpā vienosies par nepieciešamā uzdevuma izpildes nosacījumu sadali, tai skaitā par finansējuma pieprasīšanu, tādēļ finansējuma sadale pa institūcijām ir indikatīva. Finansējuma sadale pa institūcijām neietver līdzekļu pieprasījumus, kas norādīti pamatnostādņu 3.pielikumā (informācija dienesta vajadzībām). Ailē „Nepieciešamais finansējums (indikatīvi) un tā avoti" minētais finansējums ir indikatīvs, un tajā ir iespējamas izmaiņas līdz ar ES struktūrfondu un Kohēzijas fonda 2014.-2020.gada plānošanas dokumentu apstiprināšanu.

- Atbilstoši pamatnostādņu mērķiem plānojumā ir ietverti darba uzdevumi no Ministru kabinetā 2013.gada 14.oktobrī apstiprinātajām Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam (turpmāk – ISAP). Atbilstoši ISAP kā attiecīgo darba uzdevumu izpildes termiņš saglabāts 2020.gads, paredzot 2018.gadā izskatīt progresu pamatnostādņu „Latvijas kiberdrošības stratēģija 2014.-2018.gadam" īstenošanas kontekstā. Uzdevumi, kuri pārņemti no ISAP, pamatnostādnēs ir norādīti ar zemsvītras atsauci.

- Aizsardzības ministrijai sadarbībā ar visām iesaistītajām ministrijām un Nacionālo informācijas tehnoloģiju drošības padomi līdz 2016.gada 1.februārim jāiesniedz Ministru kabinetā informatīvais ziņojums par pamatnostādņu rīcības plānā noteikto uzdevumu ieviešanas gaitu, bet līdz 2019.gada 1.jūnijam – informatīvais ziņojums par pamatnostādņu rīcības plāna īstenošanas gala novērtējumu, iekļaujot priekšlikumus kiberdrošības politikas jomā turpmākajiem gadiem.

1.tabula

Kiberdrošības stratēģijas mērķu sasniegšanas uzdevumi un atbildību sadalījums

Pamatnostādnēs definētais politikas mērķis	Kiberdrošības politikas mērķis ir droša un uzticama kibertelpa, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana

1. KIBERDROŠĪBAS PĀRVALDĪBA UN RESURSI: **Nacionālā kiberdrošība**

Uzdevumi un galvenie pasākumi izvirzītā mērķa sasniegšanai	**Izpildes termiņš**	**Atbildīgā institūcija**	**Iesaistītās institūcijas**	**Nepieciešamais finansējums (indikatīvi) un tā avoti; komentāri par uzdevuma izpildi**	**Sasniedzamais politikas rezultāts un rezultatīvais rādītājs (ja iespējams)**
1.1. IKT drošības stiprināšana Latvijas prezidentūrai ES Padomē	2015.g. 2.cet.	AIM	CERT.LV, VARAM ĀM, LPESPS	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Nepārtraukts Latvijas prezidentūrai ES Padomē nepieciešamo pakalpojumu nodrošinājums, novērsti incidenti vai mazinātas to ietekmes sekas
1.2. Nacionālās kiberdrošības pārvaldības modeļa izvērtējums	2015.g. 4.cet.	AIM	NITDP iesaistītās institūcijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Uzlabots valsts institūciju sadarbības un koordinācijas modelis kiberdrošības politikas īstenošanā, iesaistot nevalstisko sektoru
1.3. Nacionālās kiberdrošības risku un spējuizvērtējums, saskaņojot to ar valsts apdraudējuma analīzi	2016.g. 1.cet.	AIM	NITDP iesaistītās institūcijas, nozares asociācijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi. *Izvērtējums tiks saskaņots NITDP*	Publiski pieejams Latvijas kibertelpas drošības pārskats, kurā ir identificēti galvenie riski un spējas
1.4. Pārvaldības modeļa izvērtējums elektronisko sakaru komersantu drošības prasību īstenošanas uzraudzībai	2017.g. 4.cet.	AIM/ SM	VP	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Skaidri definēts atbildību sadalījums par elektronisko sakaru komersantu uzraudzību saistībā ar IT drošības likumā noteikto prasību īstenošanu
1.5. Izvērtējuma izstrāde par nepieciešamību pilnveidot esošos elektronisko sakaru maģistrālos tīklus*	2018.g. 1.cet.	SM	-	*Vērtējot veicamā uzdevuma apjomu, ir konstatēts, ka būs nepieciešama ārējo konsultantu piesaiste un pētījuma veikšana. Darba apjoms un finansējuma summa būs zināma tikai ap*	Esošo elektronisko sakaru maģistrālo tīklu pilnveides nepieciešamības izvērtējums

				2016.,2017.gadu, ņemot vērā privāto komersantu attīstību un veiktās investīcijas šajā jomā	
1.6. Esošās elektronisko sakaru tīklu infrastruktūras kartēšana[13]	2018.g. 2.cet.	SM	-	Papildus nepieciešamais valsts budžeta finansējums –3 414 912 EUR	Vienota elektronisko sakaru tīklu infrastruktūras karte
1.7. Regulāra un aktīva NVO un privātā sektora partneru iesaiste NITDP darbā	Pastāvīgi	AIM	NITDP iesaistītās institūcijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	NVO pārstāvji vismaz reizi pusgadā piedalās NITDP sēdēs
1.8. Nacionālās IT drošības padomes sekretariāta darbības nodrošināšana	Pastāvīgi	AIM	-	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Padomes sekretariāts nepārtraukti nodrošina NITDP darbu un uztur komunikāciju ar Padomes locekļiem
1.9. 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

1. KIBERDROŠĪBAS PĀRVALDĪBA UN RESURSI: **Valsts IKT pārvaldība**					
1.10. Agrās brīdināšanas sistēmas izveide	2016.g. 1.cet.	CERT.LV, AIM	Valsts pārvaldes un tās pakļautībā esošas iestādes	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Izveidota agrās brīdināšanas sistēma
1.11. Publiskās pārvaldes informācijas sistēmu risku novērtējums un analīze; attiecīga sistēmu grupēšana un diferencētu drošības pārvaldības prasību ietvara izstrāde	2017.g. 4.cet.	VARAM	Latvijas Pašvaldību savienība	Tiks īstenots atbilstoši ES struktūrfondu līdzekļu sadalei	Izstrādāts diferencēts publiskās pārvaldes informācijas sistēmu modelis
1.12. Latvijas centralizētās IKT drošības un profilakses platformas izveide	2020.g. 4.cet.	VARAM	CERT.LV, AIM	Tiks īstenots atbilstoši ES struktūrfondu līdzekļu sadalei	Centralizētas IKT drošības un profilakses platformas izveide

[13] Uzdevumstermiņš un finansējums atspoguļots atbilstoši Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam;

1.13. Plašāka eID pielietošanas e-autentifikācijā nodrošināšana un bezmaksas e-Paraksta ieviešana	2018.g. 4.cet.	SM	VARAM, IEM IC, PMLP	Papildus nepieciešamais valsts budžeta finansējums – 1 900 000 EUR gadā	Plašāka eID iekļaušana e-autentifikācijas mehānismos, bezmaksas e-Paraksta ieviešana un plašāka e-paraksta pielietošana
1.14. Valsts IKT drošības pārvaldības pasākumu atskaitīšanās mehānisma izveide, izvērtējot uzraudzības efektivitāti, atbildību un soda sankcijas	2017.g. 4.cet.	VARAM	VP	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Informatīvais ziņojums par valsts IKT drošības pārvaldības modeļa pilnveidi
1.15. Valsts pārvaldes iestāžu vadības līmeņa personāla apmācību programmas metodikas izstrāde un īstenošana	2018.g. 4.cet.	Valsts kanceleja	AIM, CERT.LV, IZM	Papildus nepieciešamais valsts budžeta finansējums – 20 000 EUR. *Izmaksas ietver apmācību programmas un metodikas izstrādi (1400 EUR) un 600 personu apmācības (viena persona – 31 EUR)*	Izstrādāta un īstenota apmācību programma valsts pārvaldes iestāžu vadības līmeņa personālam
1.16. E-ID platformas modernizācija, veicot publiskās pārvaldes IKT centralizētu platformu izveidi	2018.g. 4.cet.	VARAM	SM, IEM IC, PMLP, LVRTC	Tiks īstenots saskaņā ar ES struktūrfondu līdzekļu sadali	Centralizētas publiskās pārvaldes IKT platformas izveide
1.17. Valsts pārvaldes iestāžu informēšana par nepieciešamību nodrošināt personas datu apstrādes drošību interneta vidē[14]*	2020.g. 4.cet.	TM	DVI, VARAM, CERT.LV	Papildus nepieciešamais valsts budžeta finansējums – 17 075 EUR *(līdz 2020.gadam)*	Organizēti vismaz divi semināri gadā valsts pārvaldes iestādēm par datu apstrādes drošību interneta vidē
1.KIBERDROŠĪBAS PĀRVALDĪBA UN RESURSI: **<u>Cilvēkresursi</u>**					
1.18. Profesiju standartu aktualizācijas, jomas	2015.g. 4.cet.	IZM	LM, LIKTA, LDDK,	Likumā par valsts budžetu kārtējam gadam	Profesiju standarts papildināts ar speciālistu informācijas un komunikācijas tehnoloģiju

[14]* Uzdevuma termiņš un finansējums atspoguļots atbilstoši Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam

speciālistiem nepieciešamo profesionālo kompetenču, zināšanu un prasmju kopumu IKT drošības jautājumos			LTRK, ISACA	paredzētie finanšu līdzekļi	drošības jautājumos profesionālo kompetenču sarakstu
1.19. Augsti kvalificētu vadītāju sagatavošana kiberdrošības jomā, izveidojot atbilstošas studiju izglītības programmas	2018.g. 4.cet.	AIP	Augstskolas CERT.LV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Studiju izglītības programmas izveide kiberdrošības jomā
1.20. Pedagogu profesionālās kompetences paaugstināšanas kurss IKT drošības jautājumos	2018.g. 4.cet.	IZM	VISC, CERT.LV, Latvijas Informātikas skolotāju asociācija	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Profesionālās kompetences paaugstināšanas kursu IKT drošības jautājumos noklausījušies 50 % no visiem Latvijas pedagogiem[15]
1.21. Izvērtējums un tiesību aktu pilnveide saistībā ar minimālajām kompetencēm atbildīgajām personām, kuras īsteno informācijas tehnoloģiju drošības pārvaldību valsts un pašvaldību institūcijām	2018.g. 4.cet.	VARAM	LIKTA, ISACA, CERT.LV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Informatīvais ziņojums par tiesību aktu pilnveides nepieciešamību saistībā ar minimālajām kompetencēs par drošību atbildīgajām personām
1.22. Pašnovērtējuma kompetenču vadlīnijas, kuru rezultātā iespējams konsolidēt mācību vajadzības	2018.g. 4.cet.	VARAM	LIKTA, ISACA	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Izstrādātas pašnovērtējuma kompetenču vadlīnijas

1. KIBERDROŠĪBAS PĀRVALDĪBA UN RESURSI: **Kritiskā infrastruktūra**
Informācija par 1.23., 1.24., 1.25., 1.26. un 1.27. uzdevumu pieejama pamatnostādņu 3.pielikumā (dienesta vajadzībām)

[15] 2012./2013.mācību gadā Latvijā bija 28 221 pedagogs. Avots: IZM „Aktualitātes un jaunumi izglītības jomā 2013./2014.mācību gadā"

2. TIESISKUMS KIBERTELPĀ UN KIBERNOZIEDZĪBAS MAZINĀŠANA					
Uzdevumi un galvenie pasākumi izvirzītā mērķa sasniegšanai	**Izpildes termiņš**	**Atbildīgā institūcija**	**Iesaistītās institūcijas**	**Nepieciešamais finansējums (indikatīvi) un tā avoti; komentāri par uzdevuma izpildi**	**Sasniedzamais politikas rezultāts un rezultatīvais rādītājs**
2.1. Policijas kapacitātes palielināšana	2015.g. 4.cet.	VP	IEM	Saskaņā ar Organizētās noziedzības novēršanas un apkarošanas plāna 2014.-2016.gadam" projekta (VSS-18) 2.7.p. plānoti 472 856 EUR	Palielināta policijas ekspertīze, izmeklējot noziedzīgus nodarījumus pret IKT
2.2. Kiberdrošībā lietoto terminu definīciju izstrāde latviešu valodā	2015.g. 3.cet.	IZM	VVC, LZA TK	Papildus nepieciešamais valsts budžeta finansējums – 4 000 EUR	Izstrādātas kiberdrošībā lietoto terminu definīcijas latviešu valodā
2.3. Eiropas Parlamenta un Padomes direktīvas 2013/40/ES par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes pamatlēmumu 2005/222/TI, pārņemšana	2015.g. 3.cet.	TM	VP, citas iesaistītās institūcijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Eiropas Parlamenta un Padomes direktīvas pārņemšana
2.4. Policijas darbiniekiem, prokuroriem un tiesnešiem nepieciešamās apmācības identificēšana un realizēšana	2018.g. 1.cet.	TM, VP	ĢP	*Policijas darbinieku, prokuroru un tiesnešu apmācības veicamas, pirms tam TM un VP vienojoties par apmācību jomām katrai no mērķa grupām, apmācību metodiku, nosakot apmācību īstenotāju. Uz tā pamata tiks izstrādāts detalizēts uzdevuma ieviešanas aprēķins*	Izstrādāts un īstenots policijas darbinieku, prokuroru un tiesnešu apmācības plāns
2.5. Vienota noziedzīgu nodarījumu	2016.g. 1.cet	IEM IC, TM	VP	*Vienota noziedzīgu nodarījumu elektroniskajā vidē apkopošanas*	Izveidots vienots noziedzīgu nodarījumu

kibertelpā apkopošanas mehānisma (statistikas) izveide policijas, prokuratūras un tiesu sistēmā				*mehānisma izveide veicama, pirms tam IEM IC un TM definējot tā principus, tehniskos nosacījumus, sasaisti ar VP vajadzībām. Uz tā pamata tiks izstrādāts detalizēs uzdevuma ieviešanas aprēķins*	elektroniskajā vidē apkopošanas mehānisms
2.6. Izvērtējums par Krimināllikuma un Latvijas Administratīvo pārkāpumu kodeksa regulējuma atbilstību IKT nozares normatīvajiem aktiem	2016.g. 1.cet.	TM	IEM, VARAM, SM, LIKTA, LDDK, LTRK, ISACA	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Izvērtējums par IKT nozares normatīvo aktu piemērošanas iespējām Krimināllikumam un Administratīvo pārkāpumu kodeksam
2.7. Uzraudzība, lai IS pārziņi savās darbībās ar personas datiem ieviestu un nodrošinātu augsta līmeņa aizsardzības pasākumus[16]	2017.g. 2.cet.	DVI	-	Papildus nepieciešamais valsts budžeta finansējums –896 100 EUR *(līdz 2020.gadam)*	Izstrādāts informācijas sistēmu pārziņu uzraudzības mehānisms
2.8. Regulārs sadarbības formāts ar dažādām starptautiskajām kibernoziedzības apkarošanas struktūrām	2018.g. 4.cet.	VP	-	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Regulāra sadarbība ar starptautisko kibernoziedzības apkarošanas struktūru ekspertiem un speciālistiem

3. SAGATAVOTĪBA UN RĪCĪBSPĒJAS KRĪZES SITUĀCIJĀ					
Uzdevumi un galvenie pasākumi izvirzītā mērķa sasniegšanai	**Izpildes termiņš**	**Atbildīgā institūcija**	**Iesaistītās institūcijas**	**Nepieciešamais finansējums (indikatīvi) un tā avoti; komentāri par uzdevuma izpildi**	**Sasniedzamais politikas rezultāts un rezultatīvais rādītājs (ja iespējams)**

[16] Uzdevumsjāskata saistībā ar Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam;

3.1. IKT drošības stiprināšana Ārlietu ministrijā, gatavojoties Latvijas prezidentūrai ES Padomē	2014.g. 4.cet.	ĀM	-	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Drošības risinājumu pilnveide un informācijas tehnoloģiju stiprināšana pirms gaidāmās Latvijas prezidentūras ES Padomē
3.2. Ārkārtas situāciju valsts elektronisko sakaru tīkla (ĀSVEST) izveide	2014.g. 4.cet.	SM	-	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	ĀSVEST izveide
3.3. Valsts elektronisko sakaru pakalpojumu centra (VESPC) izveide	2016.g. 4.cet.	SM, VARAM	ĀM, IEM IC	*VESPC izveides organizatoriskais un tehniskais modelis (datu centru skaits un izvietojums, rezervēšanas risinājums, koordinācija nacionāla līmeņa elektronisko sakaru tīklu slēgumiem u.tml.) izstrādājams, pirms tam SM sadarbībā ar VARAM definējot tā vietu un uzbūvi vienotajā valsts IKT arhitektūrā, kā arī radot iespēju VESPC izveidošanai piesaistīt ES struktūrfondu līdzekļus*	VESPC izveide
3.4. Iekšlietu ministrijas rezerves datu centra risinājuma izveide	2016.g. 2.cet.	IEM IC, VARAM	-	Papildus nepieciešamais valsts budžeta finansējums – 550 000 EUR *IeM datu centra rezervēšanas risinājuma organizatoriskais un tehniskais modelis (datu centru skaits un izvietojums, koordinācija nacionāla līmeņa elektronisko sakaru tīklu slēgumiem u.tml.) izstrādājams vienotās valsts IKT arhitektūras izstrādes ietvarā, radot iespēju šī risinājuma izveidošanai piesaistīt ES struktūrfondu līdzekļus*	Izveidots Iekšlietu ministrijas rezerves datu centra risinājums

3.5. ĀM sakaru serviss nepārtrauktas darbības nodrošināšanai	2016.g. 4.cet.	ĀM	-	Papildus nepieciešamais valsts budžeta finansējums – 450 000 EUR	Izveidots ĀM sakaru serviss
3.6. Satelīttelefona pakalpojuma īre visās Latvijas Republikas diplomātiskajās pārstāvniecībās	2018.g. 1.cet.	ĀM	-	Papildus nepieciešamais valsts budžeta finansējums – 60 000 EUR gadā	Nodrošināts satelīttelefona pakalpojums
3.7. ĀM informācijas sistēmas līdz Dienesta vajadzībām ieskaitot, izveidošana	2014.g. 4.cet.	ĀM	-	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Informācijas sistēmas izveide
3.8. Izvērtējums par nacionālā virtuālā ārējā perimetra stiprināšanu	2017.g. 4.cet.	SM	AIM, VARAM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Informatīvais ziņojums par nacionālās virtuālā ārējā perimetra stiprināšanu, lai apzinātu, kategorizētu un izvērtētu riskus, kā arī savstarpēji koordinētu un veiktu nepieciešamos uzlabojumus
3.9. Satelīta datu pārraides risinājums starp ĀM CA un PP ES (Brisele)	2020.g. 4.cet.	ĀM	-	Papildus nepieciešamais valsts budžeta finansējums – 107 500 EUR gadā *(līdz 2020.gadam)*	Nodrošināts satelīta datu pārraides risinājums
3.10. Attīstīt un stiprināt NBS informācijas tehnoloģijas un sakaru sistēmas	2018.g. 4.cet.	NBS	AIM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Attīstītas un nostiprinātas NBS informācijas tehnoloģijas un sakaru sistēmas
3.11. Baltijas valstu un EUCOM sadarbībā un krīzes situācijas vingrinājumi	Pastāvīgi	AIM	ĀM, NBS KAV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Vismaz reizi gadā īstenots kopējs krīzes situācijas vingrinājums
Informācija par 3.12., 3.13., 3.14. un 3.15. uzdevumu pieejama pamatnostādņu 3.pielikumā (dienesta vajadzībām)					

4. SABIEDRĪBAS IZPRATNE, IZGLĪTĪBA UN PĒTNIECĪBA					
Uzdevumi un galvenie pasākumi izvirzītā mērķa sasniegšanai	**Izpildes termiņš**	**Atbildīgā institūcija**	**Iesaistītās institūcijas**	**Nepieciešamais finansējums (indikatīvi) un tā avoti; komentāri par uzdevuma izpildi**	**Sasniedzamais politikas rezultāts un rezultatīvais rādītājs (ja iespējams)**
4.1. Ikgadēja starpinstitūciju darba un pasākumu plāna izstrāde un īstenošana sabiedrības informēšanai un izpratnes veidošanai par kiberdrošības jautājumiem	Pastāvīgi	AIM	VARAM, IEM, IZM, LIKTA, LIA, LKA, CERT.LV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Darba un pasākumu plāns, kas tiek prezentēts kalendārā gada pirmajā NITDP sēdē
4.2. Akadēmis ko studiju un pētniecības attīstīšana kiberdrošības, informācijas drošības, IKT drošības jomās	2016.g. 3.cet.	IZM	Augstskolas, CERT.LV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Palielinājies akadēmisko pētījumu skaits kiberdrošības, IT un IKT drošības jomā
4.3. Projekta izstrāde IKT drošības laboratorijas izveidei	2018.g. 4.cet.	AIM	CERT.LV, IZM, LU MII	Papildus nepieciešamais valsts budžeta finansējums –50 000 EUR	Izstrādāts projekts IKT drošības laboratorijas izveidei
4.4. Lieljaudas skaitļošanas (superdatora) resursa attīstīšana	2018.g. 4.cet.	LU MII	Augstskolas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Izstrādāts darbu plāns lieljaudas skaitļošanas resursa attīstīšanai
4.5. Elektronis ko ziņojumu līnijas par pārkāpumiem internetā nodrošināšana[17]	2020.g. 4.cet.	AIM, CERT.LV	LM, LIA	Papildus nepieciešamais valsts budžeta finansējums –262 095 EUR *(līdz 2020.gadam)*	Turpmāka elektronisko ziņojumu līnijas darbības nodrošināšana
4.6. Sabiedrība s zināšanu pilnveide par IKT drošības aspektiem (E-prasmju nedēļa, kiberdrošības	2020.g. 4.cet.	VARAM	AIM, CERT.LV, LIKTA, LIA	5 741 739 EUR *NAP 2020 uzdevums „Digitālā satura un citu produktu veidošana un e-pakalpojumu attīstība, paplašinot pakalpojumu*	Palielinājies cilvēku skaits, kuri ir piedalījušies IKT drošības aspektu pasākumos, piemēram, E-prasmju nedēļas aktivitātēs iesaistījušies 70 000 cilvēku

[17]Uzdevums jāskata saistībā ar Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam

mēnesis, drošāka interneta diena)*				*pieejamības un izmantošanas iespējas ekonomiskajā darbībā, kā arī iedzīvotāju e-prasmju pilnveide" (415.rindkopa), darbība: Iedzīvotāju e-prasmju pilnveide*	
4.7. Sabiedrība s informēšana par sociālo drošību internetā – par iespējamajiem riskiem un apdraudējumiem[18]	2020.g. 4.cet.	VARAM	AIM, CERT.LV, LM, VBTAI, LIA	Papildus nepieciešamais valsts budžeta finansējums –296 244 EUR *(līdz 2020.gadam)*	Vienotas informatīvo materiālu par kiberdrošību bibliotēkas izveide
4.8. Sabiedrība s informēšana par personas datu apstrādes drošību interneta vidē (informatīvie bukleti, semināri, diskusijas, u.c.)*	2020.g. 4.cet.	TM	DVI, VARAM, CERT.LV	Papildus nepieciešamais valsts budžeta finansējums –75 984 EUR *(līdz 2020.gadam)*	Vienotas informatīvo materiālu par kiberdrošību bibliotēkas izveide
4.9. Atbalsts ja unu produktu un tehnoloģiju izstrādei*	2020.g. 4.cet.	EM	LIAA	154 450 000 EUR (t.sk. ERAF finansējums 79 220 000 EUR un privātais līdzfinansējums 75 220 000 EUR *Iepriekš minētais ir kopējais (publiskais / privātais) aktivitātē plānotais finansējums. Uz pasākumiem IKT drošības jomā var attiekties tikai daļa no norādītā finansējuma*	Jaunu IKT drošības risinājumu izveide valsts un/vai nevalstiskajā sektorā

[18]Uzdevums jāskata saistībā ar Informācijas sabiedrības attīstības pamatnostādnēm 2014.-2020.gadam

5. STARPTAUTISKĀ SADARBĪBA					
Uzdevumi un galvenie pasākumi izvirzītā mērķa sasniegšanai	**Izpildes termiņš**	**Atbildīgā institūcija**	**Iesaistītās institūcijas**	**Nepieciešamais finansējums (indikatīvi) un tā avoti; komentāri par uzdevuma izpildi**	**Sasniedzamais politikas rezultāts un rezultatīvais rādītājs (ja iespējams)**
5.1. Baltijas valstu CERT vienību saprašanās memorands	2014.g. 4.cet.	CERT.LV	AIM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Baltijas valstu CERT vienību saprašanās memoranda noslēgšana
5.2. Kiberdrošī bas ekspertu un politikas veidotāju konsultācijas Baltijas un NB8 sadarbības formātos	Pastāvīgi	AIM	ĀM, SM, CERT	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Vismaz reizi gadā organizētas Baltijas un NB8 kiberdrošības ekspertu konsultācijas
5.3. Sadarbība ar starptautiskām kompānijām, kuras ir nozīmīgas Latvijas IT vidē	Pastāvīgi	AIM	ĀM, CERT.LV	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Izveidots sadarbības formāts ar vairākām starptautiskām kompānijām
5.4. Dalība ES Draugu grupā par kiberjautājumiem	Pastāvīgi	AIM	ĀM, SM, IEM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Regulāra Latvijas pārstāvja dalība ES Draugu grupas par kiberjautājumiem sanāksmēs
5.5. Dalība ENISA	Pastāvīgi	AIM	SM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Latvijas pārstāvība ENISA darbā un sanāksmēs
5.6. Līdzdalība starptautiskās iniciatīvās un platformās[19]	Pastāvīgi	ĀM, SM, AIM, VARAM	Visas valsts pārvaldes institūcijas	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Regulāra Latvijas pārstāvja dalība starptautiskās iniciatīvās un platformās
5.7. Starptautis kas kiberdrošības mācības	Pastāvīgi	AIM	CERT.LV, NBS	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Vismaz divreiz gadā Latvijas speciālistu dalība starptautiskās kiberdrošības mācībās
5.8. Plašāka valstu loka pievienošanās starptautisko tiesību instrumentiem, piemēram, Eiropas Padomes konvencijai	Pastāvīgi	ĀM	AIM	Likumā par valsts budžetu kārtējam gadam paredzētie finanšu līdzekļi	Aicinājums pievienoties esošajiem starptautisko tiesību instrumentiem iekļauts Latvijas pārstāvja starptautiskās iniciatīvās un platformās darba kārtībā

[19]Interneta pārvaldības forums, *ICANN* (*Internet CorporationforAssignedNamesandNumber*), Pasaules informācijas sabiedrības samita dekādes pārskata pasākumi, Koalīcija par Interneta brīvību.

Informācija par 5.9. uzdevumu pieejama pamatnostādņu 3.pielikumā (informācija dienesta vajadzībām)

Finansiālās ietekmes novērtējums

Pamatnostādņu īstenošana notiks no valsts budžeta līdzekļiem, kā arī piesaistot ES struktūrfondu līdzekļus. Pamatnostādnēs noteikto atbalsta virzienu finansēšanai var tikt piesaistīts arī citu finanšu avotu finansējums.
Norādītais finansējums paredzēts līdz 2018.gadam, tomēr uzdevumu īstenošanai būs nepieciešams finansējums arī pēc pamatnostādņu plānošanas perioda.

2.tabula

Politikas plānošanas dokumenta ietekme uz valsts un pašvaldību budžetiem

	Turpmākie trīs gadi (EUR)		
	2014.gads	**2015.gads**	**2016.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	3 234 773	4 833 721
Izmaiņas valsts budžeta izdevumos	0	3 234 773	4 833 721
Izmaiņas pašvaldību budžeta izdevumos	0	0	0
Kopējā finansiālā ietekme:	0	- 3 234 773	- 4 833 721
Finansiālā ietekme uz valsts budžetu	0	- 3 234 773	- 4 833 721
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)	Pamatnostādņu ieviešanas rīcības plānojumā identificētais nepieciešamais valsts budžeta finansējums valsts pamatfunkciju īstenošanai norādīts 1.tabulā. 2.tabulā ietverts tikai apzinātais uzdevumu izpildei nepieciešamais valsts budžeta finansējums, kasvairākos uzdevumos pārklājas ar Informācijas sabiedrības attīstības pamatnostādnēs minētajiem aprēķiniem. Lēmums par pārējo pamatnostādņu rīcības virzienu uzdevumu 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 2017.-2018.gadā	**2017.gadā –** 4 752 025	**2018.gadā –** 2 425 417	**-**

3.tabula

Nepieciešamā valsts budžeta finansējuma indikatīvais aprēķins pa gadiem (EUR)

Pasākums (atbildīgā institūcija)	**2014.gads**	**2015.gads**	**2016.gads**	**2017.gads**	**2018.gads**	**Kopā** līdz 2018.gadam
1.6. Esošās elektronisko sakaru tīklu infrastruktūras kartēšana (SM)*	0	0	1 138 304	2 276 608	0	**3 414 912**
1.13. eID pielietošanas e-autentifikācijā veicināšana un atbalsts bezmaksas e-Parakstam (SM)	0	1 900 000	1 900 000	1 900 000	1 900 000	**7 600 000**
1.15. Apmācību programmas valsts pārvaldes iestāžu vadības līmeņa personālam metodikas izstrāde un īstenošana (VK)	0	0	20 000	0	0	**20 000**
1.17. Valsts pārvaldes iestāžu informēšana par nepieciešamību nodrošināt personas datu apstrādes drošību interneta vidē (TM)*	0	2 846	2 846	2 846	2 846	**11 384**
2.1. Policijas kapacitātes palielināšana (IEM)	0	472 856	0	0	0	**472 856**
2.2. Kiberdrošībā lietoto terminu definīciju izstrāde latviešu valodā (IZM)	0	4 000	0	0	0	**4 000**
2.7. Uzraudzība, lai IS pārziņi savās darbībās ar personas datiem ieviestu un nodrošinātu augsta līmeņa aizsardzības pasākumus (DVI)*	0	149 350	149 350	149 350	149 350	**597 400**
3.4. Iekšlietu ministrijas rezerves datu centra risinājuma izveide (IEM/VARAM)	0	275 000	275 000	0	0	**550 000**
3.5. ĀM sakaru serviss nepārtrauktas darbības nodrošināšanai (ĀM)	0	225 000	225 000	0	0	**450 000**
3.6. Satelīttelefona pakalpojuma īre visās Latvijas Republikas	0	0	60 000	60 000	60 000	**180 000**

diplomātiskajās pārstāvniecībās (ĀM)						
3.9. Satelīta datu pārraides risinājums starp ĀM CA un PP ES (Brisele) (ĀM)	0	0	107 500	107 500	107 500	**322 500**
4.3. Projekta izstrāde IKT drošības laboratorijas izveidei (AIM)	0	0	0	50 000	0	**50 000**
4.5. Elektroniskās ziņojumu līnijas par pārkāpumiem internetā nodrošināšana (AIM) *	0	43 683	43 683	43 683	43 683	**174 732**
4.7. Sabiedrības informēšana par sociālo drošību internetā – par iespējamajiem riskiem un apdraudējumiem (VARAM)*	0	49 374	49 374	49 374	49 374	**197 496**
4.8. Sabiedrības informēšana par personas datu apstrādes drošību interneta vidē (informatīvie bukleti, semināri, diskusijas u.c.) (TM)*	0	12 664	12 664	12 664	12 664	**50 656**
1.23.-1.27. uzdevums (dienesta vajadzībām)	0	100 000	100 000	100 000	100 000	**400 000**
3.15.uzdevums (dienesta vajadzībām)	0	0	750 000	0	0	**750 000**
Kopā	**0**	**3 234 773**	**4 833 721**	**4 752 025**	**2 425 417**	**15 245 936**

4.tabula

Nepieciešamā finansējuma (indikatīvi) sadalījums pa institūcijām (izņemot 1.23.-1.27. un 3.15. uzdevumu (informācija dienesta vajadzībām))

Institūcija	Summa (EUR) līdz 2018.gadam
Aizsardzības ministrija	224 732
Ārlietu ministrija	952 500
Datu valsts inspekcija	597 400
Iekšlietu ministrija	1 022 856
Izglītības un zinātnes ministrija	4 000
Satiksmes ministrija	11 014 912
Tieslietu ministrija	62 040
Vides aizsardzības un reģionālās attīstības ministrija	197 496
Valsts kanceleja	20 000