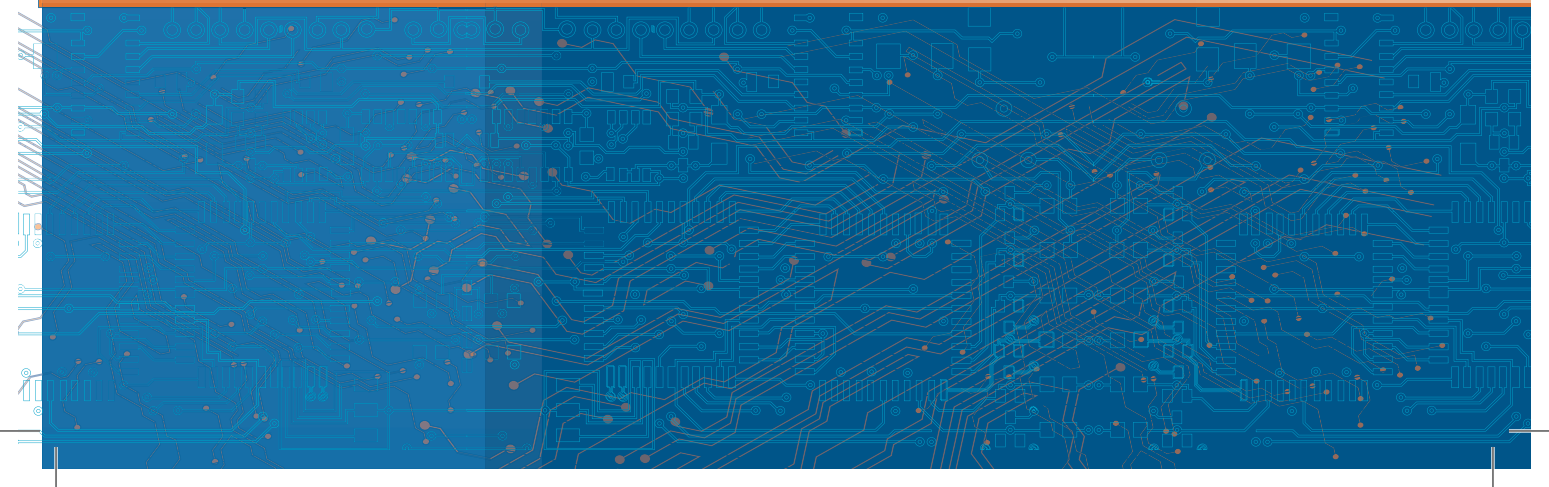
LATVIJAS KIBERDROŠĪBAS STRATĒĢIJA

2014–2018



(Ministru kabineta
2014. gada 21. janvāra
rīkojums Nr. 40)

LATVIJAS KIBERDROŠĪBAS STRATĒĢIJA

2014–2018

Saturs

1. Ievads

Latvijā ir izveidojusies informācijas sabiedrība, kurā valsts pārvalde, sabiedrība un ekonomika ir atkarīga no informācijas un komunikāciju tehnoloģiju (IKT) sniegtajām iespējām un 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 pieaugošo IKT 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 pieaug elektronisko 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.

[1] Latvijas ilgtspējas attīstības stratēģija līdz 2030.gadam.

[2] *Symantec* 2013. gada Interneta drošības draudu ziņojums par uzbrukumu un ievainojamības pieaugumu pasaulē.

2. Politikas mērķi un pamatprincipi

Kiberdrošības politikas mērķis ir droša un uzticama kibertelpa, 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 pilnveidojot prasmes IKT nozarē un tās drošības specializācijā, var efektīvi aizsargāties pret strauji pieaugošiem draudiem kibertelpā.

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 visas kibertelpā 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 sabiedrība IKT 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,[1] lielākajās Latvijas bankās elektronisko transakciju skaits ir lielāks nekā 90 % no kopējā transakciju skaita,[2] un vairāk nekā 25 % valsts institūciju pakalpojumu pieejami elektroniski.[3]

Plaša IKT izmantošana ir izmainījusi sabiedrības ikdienas paradumus, un ir izveidojusies virtuālā 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 plaši izmantotas, 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.[4] 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.

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.

[1] Centrālās statistikas pārvalde. Iedzīvotāji, kuri lieto datoru / internetu gada sākumā. 2012.

[2] Latvijas Interneta asociācija. Latvijas internetbanku pētījums. 2011.

[3] Vides aizsardzības un reģionālās attīstības ministrija. Visu valsts īstenoto publisko pakalpojumu izvērtēšanas un klasifikācijas rezultāti. Kopsavilkums par visu resoru pakalpojumiem. Versija 1.0.2012.

[4] CERT.LV 2012.gada pārskats.

4. Rīcības virzieni

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 ir iesaistīts plašs, daudzveidīgs ieinteresēto pušu loks, tāpēc nepieciešams izveidot efektīvu kiberdrošības pārvaldības modeli.

Nacionālā kiberdrošība

Nacionālā kiberdrošība 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 valsts iestāde 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. AM Nacionālās 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 konkurētspējas un 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 drošu tās lietošanu.
8. **Labklājības ministrija (LM)** īsteno sociālās un bērnu tiesību aizsardzības politiku.
9. **Latvijas Drošāka interneta centra *Net-Safe Latvia*** 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.[1]
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 un fizisko personu datu aizsardzību, taču labā prakse un standarti IKT risinājumu drošībā nav plaši izmantoti. Latvijas elektronisko sakaru komersantu tirgus ir sadrumstalots, un daļa no 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

[1] 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.

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. Pilnveidot elektronisko sakaru komersantu drošības prasību īstenošanas un uzraudzības mehānismu.
6. Pilnveidot CERT.LV spējas novērot, 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, pārskatāmi un 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.[1] 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.[2] Zināšanu un pieredzes apmaiņai, kā arī procedūru pilnveidei kritiskās infrastruktūras pārstāvji tiek regulāri iesaistīti CERT.LV rīkotās 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.

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

[2] 2011.gada 1.februāra Ministru kabineta noteikumi Nr.100 „Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība".

Cilvēkresursi

Situāciju valsts un pašvaldību institūcijās raksturo būtiski atšķirīgie cilvēkresursi un materiālie resursi, sākot no institūcijām ar labi apmaksātiem augstas kvalifikācijas darbiniekiem un moderniem tehniskajiem 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 ievēro šanu 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 mazināšanai ir 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 regulējošo normatīvo aktu bāze 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 apdraudējumi kibertelpā, 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, NBS tiek 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 nebūtu pietiekami un vienības piesaiste paātrinātu neatliekamo pasākumu īstenošanu, vai ja tās rīcībā būtu speciāli resursi šo darbību veikšanai.[1] 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 tās izmantojamību 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.
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

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

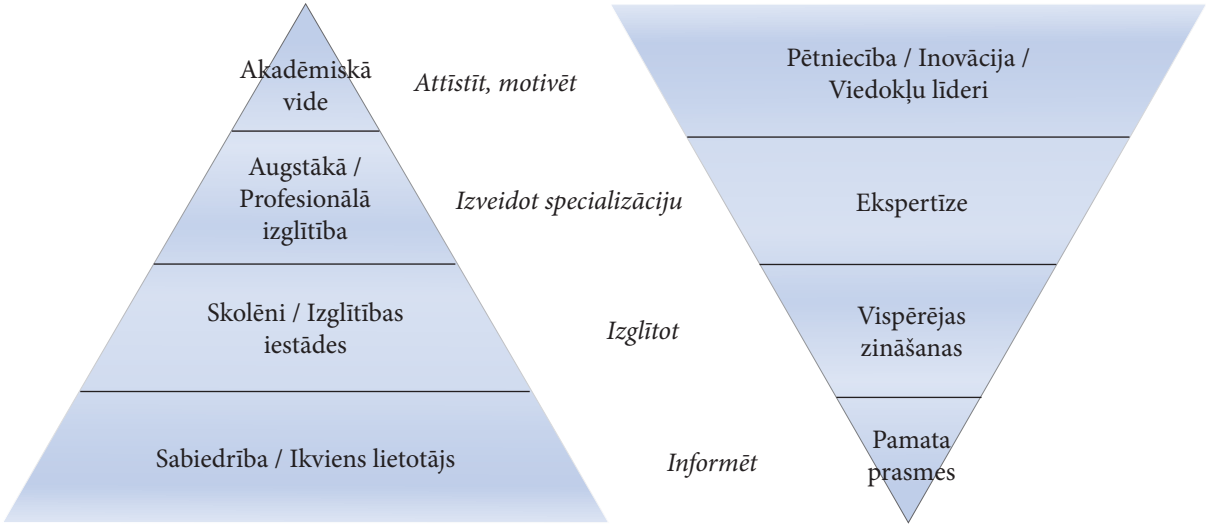
un to aizskārumiem elektroniskajā vidē, kā arī rīcību apdraudējuma gadījumā ir zems. Saskaņā ar CERT.LV rīcībā esošo statistiku gandrīz visos gadījumos, kad lietotāju iekārtas ir tikušas inficētas un kļuvušas par robotu tīklu sastāvdaļām (vidēji 15-20 tūkstoši mēnesī), lietotāji kaitējumu nav veikuši 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.).

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.[1]

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

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



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. Organizēt pedagogu 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.
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 (Freedom Online Coalition), 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 atbilstošus plānošanas 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 Direktiva 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

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
IKT	Informācijas un komunikācijas tehnoloģijas
IT	Informācijas tehnoloģijas
IZM	Izglītības un zinātnes ministrija
KAV	Nacionālo bruņoto spēku Kiberaizsardzības vienība
LB	Latvijas Banka
LM	Labklājības ministrija
LVRTC	Latvijas Valsts radio un televīzijas centrs
MIDD	Militārās izlūkošanas un drošības dienests
NATO	Ziemeļatlantijas līguma organizācija
NBS	Nacionālie bruņotie spēki
NetSafe	Latvijas Drošāka interneta centra Net-Safe Latvia
SAB	Satversmes aizsardzības birojs
SM	Satiksmes ministrija
TM	Tieslietu ministrija
VARAM	Vides aizsardzības un reģionālās attīstības ministrija
VIS	Valsts informācijas sistēmas
VP	Valsts policija
VRAA	Valsts reģionālās attīstības aģentūra

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.[1]

Kibertelpa
Kibertelpa ir interaktīva vide, kura ietver lietotājus, tīklus, skaitļošanas tehnoloģijas, programmatūru, procesus, pārsūtītas jeb uzglabātas informācijas kopumu, lietojumprogrammas, pakalpojumus un sistēmas, kas ir savienotas tieši vai netieši, izmantojot internetu, telekomunikācijas vai datortīklus, un kurā mijiedarbojas tās lietotāji. Kibertelpai nav fizisko robežu.[2]

---

[1] 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.

Kritiskā infrastruktūra

Kritiskā infrastruktūra ir Latvijā izvietoti objekti, sistēmas vai to daļas, kuras ir būtiskas svarīgu sabiedrības funkciju īstenošanas, kā arī cilvēku veselības aizsardzības, drošības, ekonomiskās vai sociālās labklājības nodrošināšanai un kuru iznīcināšana vai darbības traucējumi būtiski ietekmētu valsts funkciju īstenošanu. Informācijas tehnoloģiju kritisko infrastruktūru aizsargā, lai nodrošinātu valstij un sabiedrībai būtisku pamatfunkciju veikšanu.

[2] Starptautiskās telekomunikāciju savienības Nacionālās kiberdrošības stratēģijas rokasgrāmatas „kibertelpas" definīcija angļu valodā. *„We use the term cyberspace to describe systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks"* un ITU rekomendācijas kibertelpas apraksts *„[This] includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."* ITU-T X.1205.
Pieejams: http://ej.uz/OverviewOfCybersecurity

Valsts informācijas un komunikācijas tehnoloģijas

Ar valsts informācijas un komunikācijas tehnoloģijām šajā dokumentā atbilstoši Valsts informācijas un komunikācijas tehnoloģiju pārvaldības organizatoriskā modeļa koncepcijas tvērumam un mērķim tiek apzīmēti informācijas un komunikācijas tehnoloģiju risinājumi un pakalpojumi, kurus izmanto, veido, ievieš, uztur un ekspluatē tiešās valsts pārvaldes iestādes, kā arī to pakļautībā un pārraudzībā esošās iestādes. Attiecībā uz pašvaldībām un privāto tiesību juridiskajām un fiziskajām personām, kurām deleģēta valsts uzdevumu izpilde, valsts informācijas un komunikācijas tehnoloģiju jēdziens piemērojams uz tiem informācijas un komunikācijas tehnoloģiju risinājumiem un pakalpojumiem, kuri tiek izmantoti deleģēto valsts uzdevumu izpildei.

Pielikums Nr.1 Nacionālās kiberdrošības politikas koordinācijas shēma