**Likumprojekta „Grozījumi Informācijas tehnoloģiju drošības likumā” sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

|  |
| --- |
| **I. Tiesību akta projekta izstrādes nepieciešamība** |
| 1. | Pamatojums | Likumprojekts izstrādāts, pamatojoties uz Aizsardzības ministrijas iniciatīvu.  |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | Likumprojekts ir izstrādāts, lai1. precizētu Latvijas Universitātes aģentūras “Latvijas Universitātes Matemātikas un informātikas institūts” nosaukumu;
2. nodotu uzdevumus un tiesības, kurus šobrīd uz deleģējuma līguma pamata veic Latvijas Universitātes aģentūra “Latvijas Universitātes Matemātikas un informātikas institūta” struktūrvienība Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (turpmāk – CERT.LV), attiecībā uz Aizsardzības ministrijas (turpmāk – AM) un tās padotībā esošo iestāžu un Nacionālo bruņoto spēku (turpmāk – NBS) informācijas un komunikāciju tehnoloģijām Militārās izlūkošanas un drošības dienestam (turpmāk – MIDD);
3. CERT.LV vai MIDD būtu tiesības pieprasīt atslēgt “.lv” domēna vārdu, ja tas iesaistīts drošības incidentā.
4. Likumprojektā paredzēts precizēt Latvijas Universitātes aģentūras “Latvijas Universitātes Matemātikas un informātikas institūts” nosaukumu, jo ar Ministru kabineta 2015.gada 24.novembra rīkojumu Nr.738 “Par Latvijas Universitātes aģentūras “Latvijas Universitātes Matemātikas un informātikas institūts” pārveidi” (turpmāk – rīkojums) Latvijas Universitātes aģentūra “Latvijas Universitātes Matemātikas un informātikas institūts” pārveidots par Latvijas Universitātes zinātnisko institūtu – atvasinātu publisku personu “Latvijas Universitātes Matemātikas un informātikas institūts”. Ar rīkojumu apstiprināts Latvijas Universitātes Matemātikas un informātikas institūta nolikums, kurā noteikts, ka turpmāk pilns institūta nosaukums latviešu valodā ir Latvijas Universitātes Matemātikas un informātikas institūts.
5. Līdz ar informācijas un komunikāciju tehnoloģiju (turpmāk – IKT) jomas attīstību un šo tehnoloģiju lomas nozīmīguma pieaugumu palielinās arī apdraudējuma līmenis valsts un sabiedrības drošībai, sabiedriskajai kārtībai. Ar informācijas un komunikāciju tehnoloģiju palīdzību ir iespējams traucēt vai apturēt valsts informācijas sistēmu un elektronisko sakaru tīklu darbību, apgrūtināt valsts politisko, ekonomisko un militāro lēmumu pieņemšanas mehānismu funkcionēšanu, radot zaudējumus, dezinformējot sabiedrību.

Aizsardzības ministrijai ir deleģētas tādas funkcijas kā valsts aizsardzības politikas īstenošana, savukārt NBS mērķis ir aizsargāt Latvijas valsts suverenitāti, teritoriālo nedalāmību un tās iedzīvotājus no agresijas. Ņemot vērā aizsardzības nozares nozīmību, pastāv būtiski riski, ka uzbrukumi varētu tikt vērsti tieši pret AM un tās padotībā esošo iestāžu un NBS informācijas un komunikāciju tehnoloģijām. Pastiprinātu interesi par aizsardzības nozares informācijas un komunikāciju tehnoloģijām rada arī tas, ka Latvijā regulāri tiek rīkotas Ziemeļatlantijas līguma organizācijas (turpmāk – NATO) mācības. Atsevišķos gadījumos šīs mācības pavada mērķtiecīgi organizēti uzbrukumi IKT.NATO kiberdrošības koncepcija paredz pret apdraudējumu nodrošināt gan civilās, gan aizsardzības nozares informācijas sistēmas. Vienlaikus šajā koncepcijā ir uzsvērts to informācijas sistēmu, kuras izmanto NATO ietvaros veikto uzdevumu izpildei, nozīmīgums. Tādēļ, ņemot vērā iepriekš minētos apdraudējuma faktorus, kā arī to, ka NATO ietvaros kiberdrošība ir viens no institūciju, kas veic izlūkošanu, uzdevumiem un, lai sekmīgi, atbilstoši mūsdienu tendencēm un pastāvošajam apdraudējumam veiktu preventīvos pasākumus un spētu operatīvi reaģēt uz iespējamiem apdraudējumiem, ir nepieciešams nodrošināt specifisku un pastiprinātu drošību AM un tās padotībā esošo iestāžu un NBS informācijas un komunikāciju tehnoloģijām. Lai pilnveidotu aizsardzības nozarei piešķirto resursu izmantošanu un nodrošinātu drošu informācijas izmantošanu informācijas tehnoloģiju drošības jomā, CERT.LV uzdevumus un tiesības attiecībā uz AM un tās padotībā esošo iestāžu un NBS informācijas un komunikāciju tehnoloģijām nepieciešams nodot MIDD. Tas arī ļaus operatīvāk reaģēt uz iespējamiem apdraudējumiem. Ar likumprojekta ieviešanu Informācijas tehnoloģiju drošības likumā tiks noteikts, ka CERT.LV uzdevumus un tiesības attiecībā uz AM un tās padotībā esošo iestāžu un NBS informācijas un komunikāciju tehnoloģijām veiks MIDD, bet attiecībā uz citām valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām – CERT.LV, kā arī likumā tiks noteikts, ka abas minētās institūcijas savstarpēji apmainīsies ar to rīcībā esošo informāciju, lai nodrošinātu tām noteikto uzdevumu īstenošanu. Tādējādi tiks koncentrēti aizsardzības nozarei piešķirtie valsts resursi un pastiprināta specifisko IKT drošība.1. Likumprojketā paredzēts noteikt, ka CERT.LV vai MIDD ir tiesības pieprasīt, lai augstākā līmeņa domēna “.lv” reģistra un elektroniskās numurēšanas sistēmas uzturētājs – Latvijas Universitātes Matemātikas un informātikas institūta Tīkla risinājumu daļa (turpmāk – NIC.LV) – atslēdz augstākā līmeņa domēnā “.lv” reģistrētu domēna vārdu uz noteiktu laiku. Šādas tiesības CERT.LV vai MIDD būs gadījumā, ja domēna vārds apdraudēs IKT sistēmu drošību vai interneta lietotāju drošību.

**Likumprojekta mērķis ir novērst un mazināt apdraudējumu lietotājiem, kas tiek radīts, izmantojot augstākā līmeņa domēnā “.lv” reģistrētu domēna vārdu**. Paredzētā redakcija nosaka atslēgt domēna vārdus tajos gadījumos, kad domēna vārda lietotājs vai servera, uz kura glabājas, piemēram, ļaundabīga programmatūra vai pikšķerēšanas lapa, uzturētājs ir ļaunprātīgo aktivitāšu organizētājs un labuma guvējs. Atslēgšana ir paredzēta kā galējais līdzeklis tajos gadījumos, kad incidentu nav iespējams novērst citā veidā, piemēram, incidenta izraisītājs nereaģē uz atkārtotiem mēģinājumiem ar viņu sazināties. Noteikt šādas tiesības CERT.LV un MIDD ir nepieciešams, jo:1. **esošā kārtība domēna vārda piespiedu slēgšanai ir ilgstošs process.** Līdzšinējā praksē ir konstatēti gadījumi, kad tiek reģistrēti domēna vārdi, lai, izmantojot interneta lietotāju neuzmanību vai nezināšanu, izkrāptu lietotāju finanšu līdzekļus un informāciju vai inficētu datorus ar ļaunatūru. Esošais regulējums nosaka, ka gadījumā, ja CERT.LV konstatē, ka domēna vārds ir iesaistīts drošības incidentā, CERT.LV ziņo par to Valsts policijai. Lai atslēgtu attiecīgo domēna vārdu, Valsts policijā procesa virzītājam jāiegūst tiesneša atbalsts šādas darbības veikšanai. Līdz ar to tiesnesim procesuālajā kārtībā ir tiesības pieprasīt atslēgt domēna vārdu. IKT drošības jomā iepriekš minētais process ir neefektīvs, jo līdz brīdim, kad domēna vārds tiek atslēgts, IKT sistēmu vai interneta lietotāju drošības apdraudējums var būtiski palielināties.
2. **tas atturētu aktīvi izmantot domēna vārdus augstākā līmeņa domēnā “.lv” ļaunprātīgu rīcību veikšanai.** Iespēja atslēgt šādi izmantotus domēna vārdus preventīvi novērstu apdraudējumu pirms kaitīgā nodarījuma izdarīšanas vai vismaz mazinātu tā ietekmi un, iespējams, atturētu mērķtiecīgi veikt šādas darbības, izmantojot domēna vārdu austākā līmeņa domēnā “.lv”. Šāda atslēgšanas iespēja padarītu augstākā līmeņa domēnu “.lv” drošāku un uzticamāku sabiedrībai.

Domēna vārda slēgšana būtu nepieciešama, piemēram, šādos gadījumos: (a) ja domēna vārds tiek izmantots pikšķerēšanas nolūkos, lai izkrāptu lietotāju informāciju. Ja domēna vārda reģistrētājs vai pikšķerēšanas lapas servera uzturētājs nav iesaistīts incidentā, tad CERT.LV vai MIDD sekmīgi un ātri vienojas par attiecīgā kaitīgā resursa slēgšanu. Ja domēnu vārda reģistrētājs ir incidenta radītājs, tad nekāda sadarbība ar CERT.LV vai MIDD nenotiek, un ātrākais veids, kā aizvērt pikšķerēšanas tīmekļa vietni un apturēt informācijas noplūdi, ir atslēgt domēna vārdu. (b) ja domēna vārds tiek izmantots robotu tīklu infrastruktūrā kā komandu un kontroles centrs vai kā infekcijas posmu elements un ar to saistītie servisi ir kompromitēti un apdraud lietotāju informācijas tehnoloģiju (turpmāk – IT) drošību. Arī šajos gadījumos incidentu ir iespējams novērst vienojoties ar domēna vārda lietotāju, ja domēna vārda lietotājs tajā nav iesaistīts. Pretējā gadījumā domēna atslēgšana ir vislabākais veids, kā samazināt incidenta negatīvo ietekmi.(c) ja domēna vārds tiek izmantots ļaunatūras izplatīšanai. Ja domēna vārds tiek izmantots, lai izplatītu ļaunatūru, un tā lietotājs nav ieinteresēts sadarboties ar CERT.LV vai MIDD, lai pārtrauktu šīs darbības, atslēgšana būtu ātrākais veids, lai apturētu ļaunatūras tālāku izplatību un informētu lietotājus. Likumprojektā ir izmantots termins “atslēgšana”, ar ko, atbilstoši NIC.LV 2009.gada 1.jūlija noteikumiem “Domēna vārdu lietošanas noteikumi augstākā līmeņa domēnā “.lv”[[1]](#footnote-1), tiek saprasta domēna vārda tehniskās informācijas bloķēšana Reģistrā jeb visu “.lv” augstākā līmeņa domēnā reģistrēto domēna vārdu datu bāzē. Paredzēts, ka domēna vārda atslēgšanas pieprasījumā ir jānorāda atslēgšanas ilgums, kas nevar pārsniegt 5 dienas. Šāds termiņš ir noteikts, balstoties uz labo praksi un pieredzi citās valstīs, piemēram, Šveicē. Ja tomēr noteiktajā termiņā problēmu nav izdevies novērst un domēna vārda pieslēgšana atpakaļ atjaunotu apdraudējumu lietotājiem, CERT.LV vai MIDD var pieprasīt to atkal atslēgt. Atslēgšanas pagarināšana ir iespējama tik ilgi, kamēr problēmu izdodas novērst. Paralēli atslēgšanas procesam ITDL ir iekļauta iespēja CERT.LV vai MIDD lūgt NIC.LV veikt citas pieprasījumā norādītās darbības. Šādu iespēju ir nepieciešams iekļaut, lai atsevišķos gadījumos varētu veikt padziļinātu incidenta izpēti, kā arī novēršanu, sadarbojoties ar mitināšanas (*hosting*) pakalpojuma sniedzēju. Paredzams, ka šīs papildu darbības tiktu veiktas ar mērķi novirzīt domēna vārdu ierakstus uz CERT.LV vai MIDD infrastruktūru. Atslēgšanas gadījumā lietotāji tiek pasargāti no inficēšanās, savu datu izpaušanas u.tml., bet, ja domēna ieraksti papildus tiek novirzīti uz kontrolētu infrastruktūru, tad rodas arī iespēja uzzināt, kas mēģina slēpties aiz šiem domēna vārdiem. Reizē ir iespēja uzzināt konkrētu upuru sarakstu un viņus savlaicīgi brīdināt par kompromitētiem kontiem, noplūdušiem datiem, inficētām iekārtām.Paralēli šai incidenta novērošanai notiktu arī sazināšanās ar mitināšanas (*hosting*) pakalpojumu sniedzēju, kur attiecīgā informācija tiek glabāta, lai to noņemtu. Ja mitināšanas pakalpojumu sniedzējs pats nav ļaunprātīgs, tad 5 dienu laikā vairumā gadījumu izdotos panākt šīs informācijas noņemšanu. Ja mitināšanas pakalpojuma sniedzējs ir ļaunprātīgs, tad CERT.LV vai MIDD kompetencē ir atrasts tehnisku risinājumu, kā pasargāt lietotājus no šī incidenta atkārtošanās, ieskaitot atkārtotu atslēgšanas pieprasījumu, pieprasījumu atslēgt IP adresi (ja tā ir Latvijā) u.tml.Līdzīgas tiesības pieprasīt NIC.LV atslēgt domēna vārdu Elektronisko sakaru likumā ir noteiktas Izložu un azartspēļu uzraudzības inspekcijai, lai mazinātu nelikumīgas azartspēļu organizatoru darbības interneta vidē.Pašreizējā Informācijas tehnoloģiju drošības likuma redakcija piešķir CERT.LV tiesības uz laiku atslēgt IP adresi Latvijā, ja tā apdraud IKT sistēmu vai interneta lietotāju drošību. Ņemot vērā to, ka domēna vārdi ir līdzvērtīgs IKT resurss IP adresei, tad būtu likumsakarīgi, ja līdzvērtīgas tiesības CERT.LV un MIDD būtu arī attiecībā uz domēna vārdiem, kas reģistrēti augstākā līmeņa domēnā “.lv”. Šādu tiesību piešķiršana CERT.LV un MIDD dotu papildu iespēju pasargāt interneta lietotājus no tūlītēja apdraudējuma, kā arī uzlabot spējas cīņā ar kibernoziedzību.Arī vairākās Eiropas valstīs, kā, piemēram, Šveicē[[2]](#footnote-2) un Čehijā, drošības incidentu novēršanas institūcijām likumā ir paredzētas tiesības uz laiku atslēgt domēna vārdu, ja tas apdraud IKT sistēmu vai interneta lietotāju drošību.Līdztekus šīm izmaiņām, nepieciešams veikt grozījumus Elektronisko sakaru likumā, lai noteiktu pienākumu NIC.LV izpildīt CERT.LV vai MIDD pieprasījumu.  |
| 3. | Projekta izstrādē iesaistītās institūcijas | Projektu izstrādāja AM, MIDD un CERT.LV. Kompetenču sadalījums starp CERT.LV un MIDD ir atbalstīts Valsts drošības iestāžu padomē (padomes 2016.gada 25.janvāra protokols Nr.5.2.-16/16/1).Attiecībā uz grozījumiem par “.lv” domēna vārda atslēgšanu drošības incidentu gadījumā likumprojekta izstrādes gaitā notika konsultācijas ar NIC.LV.  |
| 4. | Cita informācija | Nav. |
|   |

|  |
| --- |
| **II. Tiesību akta projekta ietekme uz sabiedrību, tautsaimniecības attīstību un administratīvo slogu** |
| 1. | Sabiedrības mērķgrupas, kuras tiesiskais regulējums ietekmē vai varētu ietekmēt | Ikviena fiziska vai juridiska persona, kuras domēna “.lv” vārds būs iesaistīts drošības incidentā. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Nav.  |
| 3. | Administratīvo izmaksu monetārs novērtējums | Nav.  |
| 4. | Cita informācija | Nav. |

|  |
| --- |
| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** |
| Projekts šo jomu neskar. |
|  |
|  |
|  |

|  |
| --- |
| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** |
| 1. | Nepieciešamie saistītie tiesību aktu projekti | 1. Nepieciešams veikt grozījumus Ministru kabineta 2004. gada 17. augusta noteikumos Nr. 716 „Militārās izlūkošanas un drošības dienesta nolikums”, paredzot, ka MIDD funkcijas ir noteiktas arī Informācijas tehnoloģiju drošības likumā.
2. Nepieciešams veikt grozījumus Elektronisko sakaru likumā, papildinot to ar 13.3 pantu (projektam pievienots likumprojekts “Grozījums Elektronisko dokumentu likumā” un tā anotācija).
 |
| 2. | Atbildīgā institūcija | AM, MIDD, CERT.LV |
| 3. | Cita informācija | Nav. |

|  |
| --- |
| **V. Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām saistībām** |
| Projekts šo jomu neskar. |

|  |
| --- |
| **VI. Sabiedrības līdzdalība un komunikācijas aktivitātes** |
| 1. | Plānotās sabiedrības līdzdalības un komunikācijas aktivitātes saistībā ar projektu | Projekts sabiedriskajai apspriešanai publicēts Aizsardzības ministrijas mājaslapas sadaļā „Sabiedrības līdzdalība”.  |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Nav. |
| 3. | Sabiedrības līdzdalības rezultāti | Likumprojekts konceptuāli atbalstīts.  |
| 4. | Cita informācija | Nav. |

|  |
| --- |
| **VII. Tiesību akta projekta izpildes nodrošināšana un tās ietekme uz institūcijām** |
| 1. | Projekta izpildē iesaistītās institūcijas | CERT.LV un MIDD. |
| 2. | Projekta izpildes ietekme uz pārvaldes funkcijām un institucionālo struktūru. Jaunu institūciju izveide, esošu institūciju likvidācija vai reorganizācija, to ietekme uz institūcijas cilvēkresursiem | Jaunu institūciju izveide nav nepieciešama. Attiecībā uz Informācijas tehnoloģiju drošības likumā minēto uzdevumu un tiesību pārdali starp CERT.LV un MIDD, likumprojekts paredz, ka CERT.LV deleģētie Informāciju tehnoloģiju drošības incidentu novēršanas institūcijas darbības uzdevumi un tiesības, kas attiecas uz AM un tās padotības iestādēm un NBS, tiek nodoti MIDD un MIDD tos īstenos, izmantojot tam piešķirtos resursus. |
| 3. | Cita informācija | Nav. |

Aizsardzības ministrs R. Bergmanis

Vīza: Valsts sekretārs J. Garisons

L. Masāne, 67177804

linda.masane@midd.gov.lv

E. Vīksne, 67335353

elina.viksne@mod.gov.lv

Z. Beļavska, 67335354

zane.belavska@mod.gov.lv

1. Domēna vārdu lietošanas noteikumi augstākā līmeņa domēnā “.lv” <https://www.nic.lv/lv/lietosanas-noteikumi> [↑](#footnote-ref-1)
2. Rīkojums par Interneta domēniem. 15.pants. <https://www.admin.ch/opc/en/classified-compilation/20141744/index.html> [↑](#footnote-ref-2)