**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, lai   1. 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. ieviestu atbildīgas atklāšanas procesu (turpmāk – AA process) un atrunātu kārtību personu veiktai drošības nepilnību meklēšanai, atklāšanai un ziņošanai; 4. CERT.LV vai MIDD būtu tiesības pieprasīt atslēgt “.lv” domēna vārdu, ja tas iesaistīts drošības incidentā. 5. 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. 6. 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. Mūsdienu sabiedrībā IKT ir neatņemama ikdienas sastāvdaļa. Tās tiek plaši izmantotas kā saziņā un informācijas ieguvē, tā daudzu citu funkciju īstenošanā. Daudzas no šīm tehnoloģijām un sistēmām ir vitāli svarīgas sabiedrības un valsts patstāvīgai funkcionēšanai. Palielinoties tehnoloģiju daudzveidībai un skaitam, arvien grūtāk ir izsekot un novērtēt to atbilstību drošības prasībām. Digitālā vide nemitīgi attīstītās, un drošības risinājumi, kas sniedza aizsardzību vēl nesenā pagātnē, šobrīd var nebūt vairs derīgi. Sistemātiska drošības nepilnību atklāšana ir dārgs process, kas prasa augsti kvalificētus un labi atalgotus speciālistus, taču to trūkums īpaši jūtams publiskajā sektorā. Starptautiski ir pazīstams process *Responsible Disclosure Policy* vai arī *Coordinated Vulnerability Disclosure Policy*, kas paredz iespēju informācijas sistēmu vai elektronisko sakaru tīklu drošības nepilnību (turpmāk – drošības nepilnība) atklāšanā iesaistīties ikvienam interesentam, ētiskajam hakerim vai pētniekam (turpmāk – persona), paredzot iesaistīto pušu tiesības un pienākumus, veicot drošības nepilnību atklāšanu, ziņošanu, novēršanu un informācijas publiskošanu. Precīza atbildīgas atklāšanas (turpmāk – AA) procesa noteikšana un ievērošana ir ļoti svarīga, lai izslēgtu iespējamību, ka AA process tiek izmantots par aizsegu ļaunprātīgām darbībām.   Pasaules praksē AA procesu ir ieviesušas daudzas starptautiskas kompānijas, kā, piemēram, *Google*, *Microsoft*, *Facebook* u.c., bet īpaši populārs tas ir ASV privātajā sektorā. 2016. gada martā ASV Aizsardzības departaments izziņoja programmu “Uzlauz Pentagonu”[[1]](#footnote-1), kuras ietvaros aicina hakerus pieteikties atļaujai, lai programmas ietvaros varētu pārbaudīt Pentagona kiberdrošību. Valstiskā līmenī AA process kopš 2013. gada veiksmīgi darbojas Nīderlandē[[2]](#footnote-2), kur labā prakse no publiskā sektora ir pārņemta arī daudzās privātā sektora kompānijās.  Arī Latvijā līdz šim ir bijuši atsevišķi gadījumi, kuros koordinētā veidā tiek novērsta un pēc tam publiskota informācija par drošības nepilnību tajos gadījumos, kad to ir atklājusi kāda persona[[3]](#footnote-3). Tāpat šāda politika jau vairāk nekā gadu sekmīgi darbojas *Swedbank* grupā, t.sk. Latvijā[[4]](#footnote-4). Līdzšinējā gan iestāžu, gan CERT.LV pieredze rāda, ka ziņojumi no personām par drošības nepilnībām tiek saņemti aizvien biežāk, bet AA procesa ietvars ļauj iestādēm laicīgi plānot savus resursus un reakciju uz šādiem ziņojumiem.  Likumprojekta mērķis, ieviešot AA procesu, ir stiprināt kiberdrošību, atklājot un mazinot esošās drošības nepilnības un novēršot to ļaunprātīgu izmantošanu. Šī mērķa sasniegšanai ar likumprojekta apstiprināšanu tiktu dota iespēja piesaistīt pētniekus un augstas kvalifikācijas speciālistus, kas citādā veidā nebūtu pieejami. AA procesa nostiprināšana likumdošanā veicinātu sabiedrības interesi un izpratni par kiberdrošību, kā arī stimulētu valsts un pašvaldību institūcijas pievērst uzmanību savu resursu drošībai. Tāpat tas, iespējams, veicinās AA procesa plašāku izmantošanu Latvijas privātajā sektorā.  AA process likumprojektā tiek attiecināts tikai uz valsts un pašvaldību informācijas sistēmām un elektronisko sakaru tīkliem. Esošā likuma redakcija un no likuma izrietošie Ministru kabineta noteikumi[[5]](#footnote-5) regulē, kā valsts un pašvaldību institūcijas uztur un aizsargā savas informācijas sistēmas un elektronisko sakaru tīklus, tāpat, nosaka par pienākumu noteiktā laikā (90 dienās) veikt nepieciešamās darbības, ja savās sistēmās vai tīklos ir konstatēta drošības nepilnība. Likumprojekta mērķis nav regulēt komersantu informācijas sistēmas un elektronisko sakaru tīklus un uzlikt komersantiem par pienākumu labot drošības nepilnības pašiem savās sistēmās un tīklos. Komersantu un citu institūciju iesaiste AA procesā ir brīvprātīga.  Jānorāda, ka ar terminu “valsts vai pašvaldības informācijas sistēmas un elektronisko sakaru tīkli” likumprojektā tiek saprastas visas valsts un pašvaldību institūciju pārziņā vai turējumā esošās informācijas un komunikācijas tehnoloģiju sistēmas un elektronisko sakaru tīkli. Ar likumprojektā lietoto terminu “valsts un pašvaldību informācijas sistēmas” tiek saprastas arī Valsts informācijas sistēmu likumā lietotais termins “valsts informācijas sistēmas”.  Esošā likuma redakcija nosaka rīcību gadījumos, kad valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs vai drošības incidentu novēršanas institūcija konstatē drošības nepilnību. Likumprojekts paredz papildināt 6.1 pantu, lai atrunātu rīcību tajos gadījumos, kad drošības nepilnību atklāj persona, kas nav pilnvarota piekļūt valsts un pašvaldību (turpmāk – iestāde) informācijas sistēmām vai elektronisko sakaru tīkliem. Likumprojekts nosaka secīgu obligāto darbību kopumu, kas ir jāievēro AA procesa ietvaros:   1. no brīža, kad persona izlemj iesaistīties AA procesā, tai ir jāveic savu darbību fiksēšana izdarīto darbību pierādīšanai; 2. drošības nepilnības atklāšanas procesā personai, lai pierādītu konkrēto drošības nepilnību, ir jāizmanto tāds pierādījumu kopums, kas pēc iespējas mazāk ietekmē sistēmas un tajā esošās informācijas drošību (pieejamību, integritāti, konfidencialitāti); 3. atklātā drošības nepilnība ar to aprakstošo informāciju jeb pierādījumu kopumu kā atbildīgas atklāšanas ziņojums (turpmāk – AA ziņojums) ir obligāti piecu darba dienu laikā jāiesniedz CERT.LV vai MIDD. Ja persona vēlas, tā AA ziņojumu papildus var nosūtīt arī attiecīgā resursa turētājam; 4. CERT.LV vai MIDD apstiprina AA ziņojuma saņemšanu un pārbauda tajā iekļauto informāciju; 5. pēc pārbaudes CERT.LV vai MIDD informē personu par drošības nepilnības pamatotību un par konstatēto informē iestādi; 6. iestāde ziņo CERT.LV vai MIDD par drošības nepilnības novēršanu; 7. CERT.LV vai MIDD informē personu par drošības nepilnības novēršanas rezultātu; 8. persona drīkst publiskot informāciju par konstatēto drošības nepilnību tikai pēc tam, kad AA process ir noslēdzies un ir zināms drošības nepilnības novēršanas rezultāts. Šis termiņš nevar būt garāks par 180 dienām.   CERT.LV vai MIDD apstiprina drošības nepilnības novēršanas rezultātu. Drošības nepilnības novēršanas rezultāts var būt:   1. drošības nepilnības novēršana; 2. situācija, kad CERT.LV vai MIDD pēc pārbaudes neatzīst AA ziņojumā iekļauto informāciju par drošības nepilnību; 3. situācija, kad CERT.LV vai MIDD uzskata, ka konstatētās drošības nepilnības ietekme un sekas ir tik nozīmīgas, ka informācija par to ir jāpublisko nekavējoties, pirms drošības nepilnība ir novērsta; 4. situācija, kad iestāde atsakās novērst drošības nepilnību un CERT.LV vai MIDD uzskata, ka ir lietderīgi informāciju par to publiskot; 5. situācija, kad drošības nepilnība netiek novērsta noteiktajā termiņā.   Uzsākot darbības AA procesa ietvaros, nepieciešams veikt pierādījumu fiksēšanu pārbaudāmā veidā, piemēram, veicot auditācijas pierakstus. Pierādījumi ļauj pārliecināties, vai persona ir vai nav ievērojusi AA procesa kārtību. Pierādījumu fiksēšana ir jāveic līdz brīdim, kad par konstatēto drošības nepilnību ir iesniegts atbildīgas atklāšanas ziņojums CERT.LV vai MIDD vai drošības nepilnība nav konstatēta. Būtiski, ka tiklīdz kā ir atklāta drošības nepilnība, atbildīgas atklāšanas ziņojums ir jāsagatavo un jāiesniedz piecu darba dienu laikā. Pierādījumu fiksēšana ir objektīvā kontrole personām, kas nolēmušas iesaistīties AA procesā, kā arī ļauj nodrošināties pret AA procesa izmantošanu kā aizsegu ļaunprātīgām rīcībām.  Ar likumprojekta apstiprināšanu Ministru kabinetam tiek dots uzdevums izdot noteikumus atbildīgas drošības nepilnības atklāšanas, pierādījumu fiksēšanas, atbildīgas atklāšanas ziņojuma sagatavošanas, tā iesniegšanas, apstrādes par drošības nepilnību kārtības noteikšanai un informācijas publiskošanas apjoma noteikšanai.  Esošā likuma redakcija nosaka visas drošības nepilnības novēršanai nepieciešamās darbības veikt 90 dienu laikā no tās konstatēšanas brīža, tomēr likumprojektā tiek noteikts, ka attiecībā uz iesniegtajiem AA ziņojumiem visas drošības nepilnības novēršanai nepieciešamās darbības nepieciešams veikt 90 dienu laikā no brīža, kad CERT.LV vai MIDD to ir pārbaudījusi un apstiprinājusi par pamatotu un paziņojusi iestādei. Likumprojektā ir pievienota atruna gadījumiem, kad novēršanu nav iespējams veikt minētajā laikā, piemēram, ir jāveic drošības risinājumu iepirkums. Iestājoties tādai situācijai, institūcija informē CERT.LV vai MIDD par objektīvajiem iemesliem un CERT.LV vai MIDD pagarina konkrētās drošības nepilnības novēršanas termiņu, kas atbilstoši likumprojektam nevar būt ilgāks par 180 dienām no brīža, kad nepilnība ir konstatēta vai atzīta par pamatotu. Termiņš ir pagarināms tikai vienu reizi. Iepriekš minētais termiņš attieksies arī uz gadījumiem, kad valsts vai pašvaldības institūcijas, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs būs konstatējis drošības nepilnību pats savās sistēmās  Ļoti nozīmīgs AA procesa ieviešanas aspekts ir tas, ka AA procesa ieviešana radīs iespēju atbrīvot no kriminālatbildības tās personas, kuras pilnībā ievēros AA procesa nosacījumus un kārtību. Lai to nodrošinātu, ir nepieciešams veikt grozījumus Krimināllikuma 241. pantā “Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai”, izsakot trešās daļas dispozīciju šādā redakcijā: “Par šā panta pirmajā daļā paredzētajām darbībām, ja tās vērstas pret automatizētu datu apstrādes sistēmu, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību, izņemot gadījumos, kad ir ievēroti atbildīgas drošības nepilnības atklāšanas procesa nosacījumi un kārtība”. Papildinot trešo daļu ar frāzi: “izņemot gadījumos, kad ir ievēroti atbildīgas drošības nepilnības atklāšanas procesa nosacījumi un kārtība”, tiek veicināta AA procesa piemērošana, lai atbrīvotu no kriminālatbildības personas, kas Krimināllikuma izpratnē ir patvaļīgi piekļuvušas valsts vai pašvaldības informācijas sistēmai vai elektronisko sakaru tīklam (automatizētai datu apstrādes sistēmai, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību).   1. Izteikt 241.panta trešās daļas dispozīciju šādā redakcijā:   “(3)Par šā panta pirmajā daļā paredzētajām darbībām, ja tās vērstas pret automatizētu datu apstrādes sistēmu, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību, izņemot gadījumos, kad ir ievēroti atbildīgas drošības nepilnības atklāšanas procesa nosacījumi un kārtība, –  Ar likumprojektā noteikto piekļūšanu valsts un pašvaldības informācijas sistēmai vai elektronisko sakaru tīklam, ir saprotama Krimināllikuma 241.panta pirmajā daļā norādītā piekļūšana automatizētas datu apstrādes sistēmas resursiem. Normatīvie akti lieto dažādus terminus, attiecinot tos uz vienu un to pašu objektu. Krimināllikumā tiek lietots termins “automatizētas datu apstrādes sistēmas resursi”, bet Informācijas tehnoloģiju drošības likumā tiek lietots termins “valsts vai pašvaldības informācijas sistēma vai elektronisko sakaru tīkls”. Lai izveidotu sasaisti starp šiem diviem likumiem un lai tiesību piemērotājiem būtu saprotams, kādā gadījumā persona tiek atbrīvota no kriminālatbildības par piekļūšanu automatizētai datu apstrādes resursiem, tad likumprojektā tiek lietots termins “valsts un pašvaldības informācijas sistēma vai elektronisko sakaru tīkls”, reizē ar to saprotot automatizētu datu apstrādes sistēmu, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību.  Minētais nosacījums par personas atbrīvošanu no kriminālatbildības neattiecas un neregulē zaudējumu piedziņu civiltiesiskā kārtībā. Ja AA procesa ietvaros tiek nodarīti zaudējumi infrastruktūras īpašniekiem, turētājiem vai tiesiskajiem valdītājiem, tad viņiem ir tiesības vērsties pret personu civiltiesiskā kārtībā.  AA procesa ievērošanā liela atbildība gulstas uz personu, kurai ir ļoti uzmanīgi jāvērtē ikviena sava darbība, un, tiklīdz kā tiek atrasta kāda drošības nepilnība vai skaidra norāde uz to, sava darbība ir jāpārtrauc un nekavējoties jāsniedz informācija CERT.LV vai MIDD. Ja persona neapstājas, bet cenšas savākt vairāk pierādījumu un pārbaudīt drošības nepilnības ietekmi, tad tās rīcība vairs nav klasificējama kā atbildīga un persona ir saucama pie krimināllikumā noteiktās atbildības. Tāpat, personas atbildība ir izvērtēt risku, kādā informācijas sistēmā vai elektronisko sakaru tīklā tiek uzsākta drošības nepilnību meklēšana. Personai var nebūt iespēju noskaidrot, vai attiecīgā sistēma vai tīkls ir valsts vai pašvaldības institūcijas pārziņā vai turējumā, kā arī, vai tā ir vai nav automatizēta datu apstrādes sistēma, kas apstrādā informāciju, kas saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību. Līdz ar to, ja pastāv šaubas, vai attiecīgais resurss ir likumprojekta tvērumā, tad ieteicams nesākt drošības nepilnību meklēšanu AA procesa ietvaros.  Publiskošanas aspekts ir viens no būtiskākajiem AA procesa elementiem. Tas kalpo kā motivācija institūcijām nevilcināties un veikt visas nepieciešamās darbības, lai novērstu atklāto drošības nepilnību. Tomēr atbilstoši likumprojekta redakcijai persona, kas atklājusi drošības nepilnību, sadarbībā ar CERT.LV vai MIDD publiskošanu var veikt tikai pēc tam, kad AA process ir noslēdzies. Informācijas publiskošana, pirms AA process ir noslēdzies, uzskatāma par bezatbildīgu, jo tā, iespējams, kavē ātrāku tās novēršanu un rada iespēju kādam ļaunprātīgi izmantot publiskoto informāciju. Tai pašā laikā nevar izslēgt gadījumus, kad institūcijas kavēs noteiktos termiņus neobjektīvu iemeslu dēļ, vilcināsies vai ignorēs informāciju par atklāto drošības nepilnību, tādējādi pārkāpjot likumā noteiktās prasības un rīkojoties bezatbildīgi.  Personām, kas atklās drošības nepilnības AA procesa ietvaros, nav paredzēts piešķirt atlīdzību, tomēr plānots ieviest cita veida atzinības pasākumus, piemēram, izveidojot CERT.LV vai MIDD uzturētu sarakstu ar personām, kas ir veiksmīgi piedalījušās AA procesā un kuras brīvprātīgi vēlētos iekļaut savu vārdu šajā sarakstā.  AA procesa ieviešanā ir sagaidāmi vairāki izaicinājumi. Pirmkārt, AA procesa ieviešanas laikā plašs darbs būs jāfokusē uz visu iesaistīto pušu – resursu turētāju, pētnieku, tiesībsargājošo iestāžu, publiskās pārvaldes, mediju un sabiedrības – izpratnes veidošanu par AA procesa būtību un strikto kārtību. Otrkārt, ņemot vērā Latvijas situāciju ar konstanto resursu un cilvēku trūkumu publiskajā sektorā, institūcijām varētu būt sarežģīti nodrošināt laicīgu un adekvātu reakciju uz saņemtajiem AA ziņojumiem un operatīvi strādāt pie to novēršanas. Treškārt, būs nepieciešams mainīt sabiedrībā esošos priekšstatus un stereotipus. Kā liecina līdzšinējie gadījumi, saņemot informāciju par drošības nepilnībām, institūcijas to cenšas apstrīdēt, noliedz vai uztver kā apkaunojumu un pierādījumu sliktajai drošības situācijai. Šāda reakcija izriet no priekšstata, ka kiberdrošība ir statisks un 100% sasniedzams mērķis, taču digitālajā vidē tas ir praktiski neiespējami. Ir jāveicina izpratne par to, ka drošības nepilnības ir neatņemama kiberdrošības sastāvdaļa, kas turklāt konstanti mainās un attīstās. Šajā kontekstā sagaidāms, ka negatīvi tiktu vērtēts AA procesa publiskošanas aspekts, jo institūcijas to uztvertu kā draudu konkrētai infrastruktūrai, kā arī uzticamības un reputācijas risku savai iestādei vai publiskajam sektoram kopumā. Tomēr jāuzsver, ka draudus un riskus radītu nevis pati publiskošana, bet fakts par esošo drošības nepilnību, kas netiek novērsta vai arī tās esamība pati par sevi būtiski apdraud sabiedrības tiesības un intereses. Visbeidzot neviennozīmīgi tiek vērtēta hakeru jeb datorurķu darbība. Hakeru kopienas eksistē arī Latvijā, un, ieviešot praksē AA procesu, tiktu demonstrēta valsts atvērtība pret šo cilvēku zināšanām un prasmēm, ļaujot viņiem iznākt no “pelēkās zonas” un kļūt par atbildīgiem drošības nepilnību pētniekiem. Tas veicinātu abpusēju uzticību, nākotnē palīdzot veidot ar viņiem sadarbību, lai tos nepieciešamības gadījumā pilnīgāk iesaistītu valsts aizsardzībā.  AA procesa ieviešanā ir riski un tie ir pastāvīgi. AA procesā ļoti liela atbildīga gulstas kā uz personu, tā uz iestādi. Tomēr AA procesa lielākais ieguvums ir iespēja kiberdrošības uzlabošanā piesaistīt personas, kuras, labu nodomu vadītas, ir gatavas ieguldīt savu laiku un zināšanas, lai atbildīgi meklētu drošības nepilnības un par tām ziņotu. Neieviešot šo politiku, netiek izmantots sabiedrībā esošais potenciāls, ko var piesaistīt valsts kiberdrošības stiprināšanai, kā arī netiek izmantota iespēja piesaistīt kiberdrošības jomai jaunus datoru drošības entuziastus. Visbeidzot jānorāda, ka personas, kurām ir ļaunprātīgi nodomi, slēptā veidā drošības nepilnības atklāj jau šobrīd, pēc tam tās pārdodot “melnajā tirgū”, tādējādi gūstot personīgu labumu un radot papildu apdraudējumu valsts drošībai.  Ņemot vērā to, ka AA process ir attiecināms uz fiziskām personām, kuras varēs darboties šī procesa ietvaros, tad Informācijas tehnoloģiju drošības likuma 2. panta pirmajā daļā nepieciešams norādīt, ka likuma tvērums attiecas arī uz fiziskām personām, kas veic atbildīgas drošības nepilnības atklāšanas procesu.  4.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”[[6]](#footnote-6), 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[[7]](#footnote-7) 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 | Visas valsts un pašvaldību institūcijas, ikviena fiziska persona, kas vēlēsies iesaistīties drošības nepilnības atklāšanā, un ikviena fiziska vai juridiska persona, kuras domēna “.lv” vārds būs iesaistīts drošības incidentā. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Attiecībā uz AA procesa ieviešanu papildus slogu CERT.LV un MIDD varētu radīt ziņojumu apstrāde, jo sagaidāma ziņojumu skaita palielināšanās. Papildu slogs varētu rasties arī institūcijām, kuru resursos tiktu atklātas drošības nepilnības. Taču ziņojumu apstrāde un drošības nepilnību novēršana ir veicama esošo administratīvo resursu ietvaros.  Informācijas tehnoloģiju drošības likuma 6.1 panta otrā daļa, kas ir spēkā kopš 2015. gada 4. marta, nosaka, ka “valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, konstatējis drošības nepilnību, 90 dienu laikā veic visas tās novēršanai nepieciešamās darbības, kā arī par konstatēto tūlīt informē Drošības incidentu novēršanas institūciju”, līdz ar to esošā likuma kārtība jau nosaka pienākumu novērst drošības nepilnības noteiktā termiņā. Taču, ņemot vērā iespējamību, ka atklāto drošības nepilnību skaits varētu palielināties, likumprojektā ir iekļauta atruna gadījumiem, kad objektīvu iemeslu dēļ nav iespējas konkrēto drošības nepilnību novērst 90 dienās, piemēram, ir jāiegādājas papildu iekārtas vai sistēma ir jāpārprogrammē no jauna, tādēļ ir jāveic iepirkums esošā budžeta ietvaros. Tādos gadījumos CERT.LV vai MIDD pagarina konkrētās drošības nepilnības novēršanas termiņu, kas nevar būt ilgāks par 180 dienām no brīža, kad nepilnība ir konstatēta vai atzīta par pamatotu.  Informācijas tehnoloģiju drošības likuma 8. panta otrā daļa, kas ir spēkā no 2011. gada 1. februāra, nosaka, ka katras „valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā”, līdz ar to institūcijām jau ir nozīmētas atbildīgās personas, kas var reaģēt un koordinēt kā drošības incidentu, tā drošības nepilnību novēršanu. |
| 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. Aizsardzības ministrijai līdz 2018.gada 1.janvārim jāizstrādā un noteiktā kārtībā jāapstiprina Ministru kabineta noteikumi par:   atbildīgas drošības nepilnības atklāšanas, pierādījumu fiksēšanas, atbildīgas atklāšanas ziņojuma sagatavošanas, tā iesniegšanas, apstrādes kārtību un informācijas publiskošanas apjomu par drošības nepilnību.   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 Krimināllikuma 241. pantā (izsludināts 2016.gada 19.maija Valsts sekretāru sanāksmē, prot. Nr.20 3§, VSS-449). 3. 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 | Likumprojekta izstrādē attiecībā uz AA procesa ieviešanu tika iesaistīts informācijas tehnoloģiju nozares profesionālis Mg. sc. comp. Kirils Solovjovs un krimināltiesību eksperts assoc.prof., dr.iur. Uldis Ķinis. Plānotās Informācijas tehnoloģiju drošības likuma izmaiņas ir pārrunātas CERT.LV drošības ekspertu grupas sanāksmē 2016. gada 14. aprīlī, kurā gūts konceptuāls atbalsts. Tāpat AA procesa ieviešanas iniciatīva tika prezentēta  2016. gada 26. aprīļa CERT.LV seminārā “Esi drošs”. |
| 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 | Visas valsts un pašvaldību institūcijas, kurām ir vismaz viena informācijas sistēma. |
| 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

4509

19.09.2016 16:25:00

L. Masāne, 67177804

[linda.masane@midd.gov.lv](mailto:linda.masane@midd.gov.lv)

E. Vīksne, 67335353

[elina.viksne@mod.gov.lv](mailto:elina.viksne@mod.gov.lv)

Z. Beļavska, 67335354

[zane.belavska@mod.gov.lv](mailto:zane.belavska@mod.gov.lv)

1. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe [↑](#footnote-ref-1)
2. https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure [↑](#footnote-ref-2)
3. https://cert.lv/resource/show/760 un https://www.eparaksts.lv/lv/jaunumi/eparaksta-lietotajus-aicina-uz-savam-darba-stacijam-nekavejoties-atjauninat-programmaturu-eparakstitajs/ [↑](#footnote-ref-3)
4. https://www.swedbank.lv/pakalpojumi\_privatpersonam/it\_ievainojamibas\_zinojumiem/ [↑](#footnote-ref-4)
5. Ministru kabineta 2015.gada 28.jūlija noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” [↑](#footnote-ref-5)
6. Domēna vārdu lietošanas noteikumi augstākā līmeņa domēnā “.lv” <https://www.nic.lv/lv/lietosanas-noteikumi> [↑](#footnote-ref-6)
7. Rīkojums par Interneta domēniem. 15.pants. <https://www.admin.ch/opc/en/classified-compilation/20141744/index.html> [↑](#footnote-ref-7)