*Projekts*

**Ministru kabineta noteikumu projekta „Kārtība, kādā valsts un pašvaldību institūcijas nodrošina informācijas un komunikācijas tehnoloģiju sistēmu, tajā skaitā valsts informācijas sistēmu, atbilstību minimālajām drošības prasībām” sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

|  |
| --- |
| **I. Tiesību akta projekta izstrādes nepieciešamība** |
| 1. | Pamatojums | Informācijas tehnoloģiju drošības likuma 8.panta piektā daļa un Valsts informācijas sistēmu likuma 4.panta otrā daļa |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | Šobrīd Informācijas tehnoloģiju drošības likums (turpmāk – IT drošības likums) nosaka drošības prasību minimumu, kas ietver obligātu ziņošanu par informācijas tehnoloģiju drošības incidentiem, par drošības pārvaldību atbildīgo personu iecelšanu institūcijās, par nepieciešamību apmeklēt apmācības, kā arī vismaz reizi gadā veikt institūcijas informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) drošības trūkumu novēršanu. Kopš IT drošības likuma stāšanās spēkā 2011. gada 1. maijā, tajā iestrādātās prasības ir sniegušas lielu ieguldījumu, lai kopumā IKT drošības situācija valsts un pašvaldību iestādēs uzlabotos. Tomēr situācija kiberdrošības jomā valsts pārvaldē vēl joprojām ir samērā zemā līmenī, tādēļ nepieciešams nodrošināt vienmērīgi augstu minimālo drošības prasību izpildi visās valsts un pašvaldību institūcijās.2015. gada februārī ir pieņemti IT drošības likuma grozījumi, kas paredz Ministru kabinetam (turpmāk – MK) izstrādāt noteikumus IKT drošības prasībām valsts un pašvaldību iestādēs, kas iekļautu gan vispārējās drošības, gan tehniskās prasības.Nepieciešamību pēc šādiem MK noteikumiem nosaka situācija, ka pašlaik nav izstrādāts regulējums, kas noteiktu vienotus standartus valsts un pašvaldību iestādēm IKT drošības jomā, līdz ar to drošības līmenis valsts un pašvaldību IKT resursos ir ļoti atšķirīgs. Esošā Valsts informācijas sistēmu likuma (turpmāk – VIS likums), no tā izrietošo MK 2005. gada 11. oktobra noteikumu Nr. 765 „Valsts informācijas sistēmu vispārējās drošības prasības” un MK 2005. gada 11. oktobra noteikumu Nr. 764 „Valsts informācijas sistēmu vispārējās tehniskās prasības” izpildi ir iespējams efektīvi kontrolēt tikai attiecībā uz Valsts informācijas sistēmu reģistrā (turpmāk – Reģistrs) reģistrētām informācijas sistēmām (pašlaik – aptuveni 175), kas ir ļoti maza daļa no kopējā valsts un pašvaldību informācijas sistēmu skaita. Būtiski, ka tajā nav iekļautas ļoti daudzas nozīmīgas sistēmas, kurās tiek apstrādāta, glabāta un pārsūtīta gan institūcijām, gan valsts iedzīvotājiem svarīga informācija. Iemesls saistāms ar to, ka pievienošanās Reģistram ir iestāžu brīva izvēle, un, izvairoties no saistībām un pienākumiem, daudzas iestādes savas sistēmas Reģistrā nav iekļāvušas. Pēc Vides aizsardzības un reģionālās attīstības ministrijas sniegtās informācijas, pēdējo gadu laikā ir konstatēti divi gadījumi, kad sistēmu iekļaušana Reģistrā notikusi tikai pēc ilgstošām pārrunām, taču lielākās problēmas rada tas, ka Reģistram nav informācijas par visām valsts un pašvaldību turējumā esošām informācijas sistēmām, līdz ar to nav arī iespēju veikt pārrunas ar šo sistēmu turētājiem, kas paši nav izrādījuši iniciatīvu. Turklāt VIS likums neparedz konkrētas tehniskās drošības prasības, bet gan tikai uzskaita nepieciešamos dokumentus, kas nozīmē, ka katrs pārzinis pats interpretē IKT drošības „labo praksi” un ievieš vai neievieš konkrētas tehniskās prasības. Noteikumu projekts paredz ieviest vienotus minimālos standartus gan valsts informāciju sistēmām, gan pārējām valsts un pašvaldību institūciju informācijas un komunikāciju tehnoloģiju sistēmām.Kā pierāda Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (turpmāk – CERT.LV) veiktie drošības testi, IKT riski un apdraudējumi vēl joprojām ir nepietiekami apzināti un nenovērtēti lielākajā daļā valsts un pašvaldību iestāžu. Institūcijām un atbildīgajām amatpersonām nav izveidojusies skaidra izpratne par nepieciešamību aizsargāt informāciju un it īpaši sistēmas un tīklus, pa kuriem tā tiek pārraidīta. Bet, tā kā IKT pakalpojumu īpatsvars valsts pārvaldē aizvien turpina pieaugt, palielināsies arī IKT drošības draudu aktualitāte un sarežģītība. Tādēļ ir nepieciešams ieviest vienotas drošības prasības un standartus visām valsts un pašvaldību iestādēm, tajā skaitā arī valsts informācijas sistēmām. Tas palīdzētu celt minimālo drošības līmeni visās valsts un pašvaldību iestādēs un nodrošināt pietiekoši augstu izturību pret iespējamiem apdraudējumiem, ar kuriem varētu ļaunprātīgi izmantot sistēmu, veikt datu nopludināšanu trešajām personām, kā rezultātā tiktu negatīvi ietekmēta gan konkrēto institūciju, gan visas valsts pārvaldes uzticamība un reputācija.Šobrīd tik vienkārša prasība kā paroles esamība katram lietotāja kontam nav obligāta, tāpēc noteikumi ievieš šo prasību kā obligātu visām sistēmām, vienlaikus aizliedzot sistēmās tādu funkcionalitāti, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada. Skaidrojam, ka šī prasība neaizliedz ieviest vai izmantot *single-sign-on* risinājumu, ja risinājuma ietvaros netiek saglabāta un nodota tālāk pati lietotāja parole, bet gan tikai informācija par lietotāja piekļuves tiesībām. Skaidrojam arī to, ka, veidojot informācijas sistēmas, kurām paredzēts piekļūt, izmantojot interneta pārlūku programmatūru, ieteicams pieteikšanās formām, kurās tiek vadīta lietotāja parole, uzstādīt Hiperteksta iezīmēšanas valodas (*HTML)* parametru *autocomplete=off*.Turklāt šobrīd CERT.LV ir konstatējusi gadījumus, kad institūcija nav juridiski tiesīga vai tehniski spējīga labot drošības nepilnības vai funkcionalitātes defektus, ja ražotājs vai piegādātājs atsakās vai nespēj to darīt, tāpēc noteikumu projektā paredzētas iepirkumu prasības jaunām sistēmām un esošo sistēmu uzlabojumiem. Saskaņā ar šiem noteikumiem personām, kuras piedalās šādos iepirkumos, būs aizliegts līgumā iekļaut punktu, kas ierobežo Autortiesību likuma 29. panta pirmajā daļā noteiktās tiesības, līdz ar to datorprogrammas reproducēšanai, tulkošanai, adaptēšanai vai jebkādai citādai pārveidošanai un šo darbību rezultātu reproducēšanai nebūs nepieciešama īpaša autortiesību subjekta atļauja, ja vien šīs darbības (arī kļūdu labošana) ir nepieciešamas datorprogrammas lietošanai paredzētajam mērķim.Ir konstatēti gadījumi, kad sistēma tiek kompromitēta, jo pieejamie programmatūras atjauninājumi netiek uzlikti pietiekami laicīgi. Tajā pašā laikā ir manīti arī pretēji gadījumi, kad nevajadzīgu, lai arī kritisku atjauninājumu uzlikšana noved pie sistēmas funkcionalitātes degradācijas. Tādēļ noteikumu projekts paredz institūcijām tiesības un pienākumus izvērtēt pieejamo programmatūras atjauninājumu nepieciešamību.Praksē bieži vien nākas saskarties ar situāciju, kad informācijas sistēma pārstāj (nespēj) funkcionēt pēc programmatūras atjauninājumu piemērošanas, taču pārlieku lielā drošības riska dēļ nav iespējams atlikt programmatūras atjauninājumu piemērošanu.*Java* ir programmatūra, uz kuras bāzes veidotas daudzas informācijas sistēmas. Diemžēl parasti informācijas sistēmas tiek veidotas tā, ka tās ir atkarīgas no konkrētas *Java* versijas, bet drošības problēmas šajā programmatūrā tiek atklātas gana bieži. Piemēram, 2013. gadā tika atklātas vairāk kā 10 dažādas ievainojamības, kas novērtētas ar nopietnību vismaz 9,3 no 10 ballēm. Līdz ar to noteikumu projekts paredz dot iespēju sistēmas atbalsta nodrošināšanas periodā turpināt sistēmas ekspluatēšanu ar jaunākajām programmnodrošinājuma versijām.Vienlīdz svarīgi ir nodrošināt arī sistēmas auditācijas pierakstu veidošanu un uzglabāšanu vismaz 6 mēnešus (paaugstinātas drošības sistēmām – 18 mēnešus) pēc ieraksta izdarīšanas. Sistēmas auditācijas pierakstos jāglabā vismaz tāda informācija, lai jebkura piekļuve sistēmai būtu izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola adresei.Noteikumu projektā paredzētais ierobežojums izvietot sistēmu ārpus Eiropas Savienības vai Eiropas Ekonomikas zonas veidots saskaņā ar Fizisko personu datu aizsardzības likumā noteiktajiem ierobežojumiem.Ņemot vērā noteikumu projekta galveno auditoriju – tos informācijas sistēmu turētājus, kas šobrīd nav pievērsuši pietiekamu uzmanību IKT drošības jautājumiem – noteikumu projekts rakstīts tādā valodā, lai to būtu pēc iespējas vieglāk uztvert arī tiem, kas nepārzina IKT drošības teoriju.Vienlaikus apzinoties, ka pamata prasības pat nesasniegs daudzu būtisku informācijas sistēmu šā brīža drošības līmeni, noteikumu projekts paredz sistēmu dalījumu pamata un paaugstinātas drošības sistēmās. Paaugstinātas drošības sistēmām paredzēts prasīt ievērot papildu vispārējās drošības prasības un papildu tehniskās prasības. |
| 3. | Projekta izstrādē iesaistītās institūcijas | Projekta izstrādei organizēta neformāla darba grupa, kas sākotnēji izveidota 2014. gada 21. novembrī.Noteikumu projekts izstrādāts Aizsardzības ministrijā, piedaloties Satiksmes ministrijai, Vides aizsardzības un reģionālās attīstības ministrijai, Satversmes aizsardzības birojam, Militārās izlūkošanas un drošības dienestam, Drošības policijai, Valsts reģionālās attīstības aģentūrai, CERT.LV, Latvijas Pašvaldību savienībai, VAS „Latvijas Valsts radio un televīzijas centrs” un VAS „Elektroniskie sakari”.Projekts elektroniski saskaņots ar Iepirkumu uzraudzības biroju. |
| 4. | Cita informācija | Projekta ietekme uz valsts budžetu šobrīd nav aprēķināma, jo nav pieejama informācija par valsts un pašvaldību institūciju rīcībā esošo IKT sistēmu šī brīža stāvokli un nepieciešamajiem resursiem, lai izpildītu projektā paredzētās prasības. Paredzams, ka izmaksas veidos tieši sistēmu pielāgošana drošības prasībām, kā arī ārēju drošības dokumentācijas auditu un ielaušanās testu veikšana. Paredzēts, ka ielaušanās testi pirms jaunas sistēmas pieņemšanas ekspluatācijā obligāti tiks veikti gan pamata, gan paaugstinātas drošības sistēmām, taču regulāri ielaušanās testi – tikai paaugstinātas drošības sistēmām. Saskaņā ar noteikumu projekta noslēguma jautājumiem prasības par sistēmu pielāgošanu būs obligātas tikai no 2018. gada (paaugstinātas drošības sistēmām) un 2021. gada (pamata drošības sistēmām). Līdz ar to papildu izdevumi valsts un pašvaldību budžetiem līdz 2017. gadam nav paredzēti. |
|   |

|  |
| --- |
| **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 iestādes. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Izmantojot valsts piedāvātos IKT pakalpojumus vai apmainoties ar informāciju pa valsts un pašvaldību informācijas sistēmām un tīkliem, gan juridisko, gan privātpersonu sniegtajai informācijai jābūt atbilstoši aizsargātai. Vienotu minimālo drošības prasību ieviešana palīdzēs izvairīties no informācijas drošības incidentiem, mazināt to ietekmi un sekas, kā arī vairos uzticību ne tikai valsts pārvaldes spējām aizsargāt iestādei un Latvijas iedzīvotājiem svarīgu informāciju, bet arī digitālajai videi kopumā. Drošības un uzticības trūkums digitālajai videi ir viens no nozīmīgākajiem iemesliem, kādēļ tiek nepietiekami izmantots arī e-tirdzniecības potenciāls, kas varētu sniegt būtisku ieguldījumu ekonomikas izaugsmē. Līdz ar to paredzams, ka augstāki standarti valsts pārvaldē ļautu pieprasīt augstāku IKT drošības līmeni arī privātajam sektoram, kas palīdzētu attīstīt e-uzņēmējdarbību.Lai gan noteikumu projekts rakstīts tā, lai netiktu pārlieku palielināts birokrātiskais slogs, šādas prasības vienlaikus prasītu dziļāku izpratni no visām valsts un pašvaldību iestādēm, kurām ir kaut viena informācijas sistēma. Turklāt katrai iestādei būtu jāsagatavo vismaz viens dokuments, kas aprakstītu noteikumos prasītos procesus un kritērijus. Lai mazinātu administratīvo slogu, paredzēts, ka šos dokumentus varēs izstrādāt vienotus visām iestādes sistēmām, turklāt valsts tiešās pārvaldes iestādēm un pašvaldībām paredzētas tiesības apstiprināt šos dokumentus savām pakļautības iestādēm un struktūrvienībām. |
| 3. | Administratīvo izmaksu monetārs novērtējums | Pamata drošības sistēmām noteiktā drošības dokumentācijas pārbaude, kas veicama vismaz reizi gadā, (19. punkts) ir iekšēja pārbaude un tā veicama esošo administratīvo resursu ietvaros kā ikgadējs darba uzdevums.Paaugstinātas drošības sistēmām, kas pieejamas izmantojot publisku datu pārraides tīklu (34. punkts) reizi divos gados jāveic ārējs drošības dokumentācijas audits un ielaušanās tests. Pasūtot vairumā, vidējās izmaksas vienas sistēmas drošības dokumentācijas auditam un ielaušanās testam ir 10 000 *euro*. Caur publisko datu pārraides tīklu pieejamo paaugstinātas drošības sistēmu skaita valsts un pašvaldību institūcijās provizoriskais novērtējums – 200 gab. Šādas pārbaudes veicamas reizi divos gados, līdz ar to izmaksas ir 10 000 *euro* x 200 = 2 000 000 *euro* divos gados jeb 1 000 000 *euro* gadā.IT drošības likuma 8. panta otrā daļa jau šobrīd nosaka, ka katras „valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā”. Šī norma ir spēkā kopš 2011. gada februāra. Tātad katrā valsts un pašvaldības institūcijā jau šobrīd ir atbildīgā persona, kas varēs izstrādāt noteikumos paredzētos dokumentus un veikt dokumentācijas prasību īstenošanas pārbaudes, līdz ar to papildu administratīvās izmaksas iestādēm neradīsies.Turklāt CERT.LV sagatavos un publicēs noteikumos paredzēto dokumentu izstrādes vadlīnijas un paraugus, lai atvieglotu valsts un pašvaldību iestādēm dokumentu izstrādes procesu. CERT.LV arī gatava konsultēt atbildīgās personas dokumentu izstrādē. |
| 4. | Cita informācija | Nav. |

|  |
| --- |
| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** |
| **Rādītāji** | **2015. gads** | Turpmākie trīs gadi (*euro*) |
| **2016.** | **2017.** | **2018.** |
| saskaņā ar valsts budžetu kārtējam gadam | izmaiņas kārtējā gadā, salīdzinot ar valsts budžetu kārtējam gadam | izmaiņas, salīdzinot ar kārtējo (n) gadu | izmaiņas, salīdzinot ar kārtējo (n) gadu | izmaiņas, salīdzinot ar kārtējo (n) gadu |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. Budžeta ieņēmumi: | - | - | - | - | - |
| 1.1. valsts pamatbudžets, tai skaitā ieņēmumi no maksas pakalpojumiem un citi pašu ieņēmumi | - | - | - | - | - |
| 1.2. valsts speciālais budžets | - | - | - | - | - |
| 1.3. pašvaldību budžets | - | - | - | - | - |
| 2. Budžeta izdevumi: | - | - | - | - | - |
| 2.1. valsts pamatbudžets | - | - | - | - | - |
| 2.2. valsts speciālais budžets | - | - | - | - | - |
| 2.3. pašvaldību budžets | - | - | - | - | - |
| 3. Finansiālā ietekme: | - | - | - | - | - |
| 3.1. valsts pamatbudžets | - | - | - | - | - |
| 3.2. speciālais budžets | - | - | - | - | - |
| 3.3. pašvaldību budžets | - | - | - | - | - |
| 4. Finanšu līdzekļi papildu izdevumu finansēšanai (kompensējošu izdevumu samazinājumu norāda ar "+" zīmi) | X | - | - | - | - |
| 5. Precizēta finansiālā ietekme: | X | - | - | - | - |
| 5.1. valsts pamatbudžets | - | - | - | - |
| 5.2. speciālais budžets | - | - | - | - |
| 5.3. pašvaldību budžets | - | - | - | - |
| 6. Detalizēts ieņēmumu un izdevumu aprēķins (ja nepieciešams, detalizētu ieņēmumu un izdevumu aprēķinu var pievienot anotācijas pielikumā): | Projektā ietverto prasību īstenošanai nepieciešamo finansējumu institūcijām jāiekļauj priekšlikumos jaunajām politikas iniciatīvām 2017.gadam, vai arī jāizvērtē iespējas piesaistīt citus finanšu avotus. |
| 6.1. detalizēts ieņēmumu aprēķins |
| 6.2. detalizēts izdevumu aprēķins |
| 7. Cita informācija | Paaugstinātas drošības sistēmām, kas pieejamas izmantojot publisku datu pārraides tīklu (34. punkts) reizi divos gados jāveic ārējs drošības dokumentācijas audits un ielaušanās tests. Pasūtot vairumā, vidējās izmaksas vienas sistēmas drošības dokumentācijas auditam un ielaušanās testam ir 10 000 *euro*. Caur publisko datu pārraides tīklu pieejamo paaugstinātas drošības sistēmu skaita valsts un pašvaldību institūcijās provizoriskais novērtējums – 200 gab. Šādas pārbaudes veicamas reizi divos gados, līdz ar to izmaksas ir 10 000 *euro* x 200 = 2 000 000 *euro* divos gados jeb 1 000 000 *euro* gadā. Šīs izmaksas tiks segtas no līdzekļiem, kas piešķirami Aizsardzības ministrijai jauno politikas iniciatīvu ietvaros pēc tam, kad Aizsardzības ministrija saskaņā ar likumprojekta „Par vidēja termiņa budžeta ietvaru 2017., 2018. un 2019.gadam” un likumprojekta „Par valsts budžetu 2017.gadam” sagatavošanas grafikā noteiktajiem termiņiem sagatavo un iesniedz attiecīgu priekšlikumu jaunajai politikas iniciatīvai noteikumu projekta paredzēto prasību īstenošanai. |

|  |
| --- |
| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** |
| 1. | Nepieciešamie saistītie tiesību aktu projekti | Ar šo noteikumu spēkā stāšanos spēku zaudē MK 2005. gada 11. oktobra noteikumi Nr. 765 „Valsts informācijas sistēmu vispārējās drošības prasības”, jo abi noteikumi savstarpēji pārklājas, turklāt šajos noteikumos ir noteiktas augstākas un precīzākas drošības prasības gan IKT, gan valsts informācijas sistēmām. |
| 2. | Atbildīgā institūcija | Aizsardzības ministrija |
| 3. | Cita informācija | Esošais VIS likums un no tā izrietošie MK 2005. gada 11. oktobra noteikumi Nr. 764 „Valsts informācijas sistēmu vispārējās tehniskās prasības” attiecas tikai uz Reģistrā iekļautajām informācijas sistēmām, kas ir ļoti maza daļa no kopējā valsts un pašvaldību resursu skaita. Tajā nav iekļautas ļoti daudzas nozīmīgas sistēmas, kurās tiek apstrādāta, glabāta un pārsūtīta gan institūcijām, gan valsts iedzīvotājiem svarīga informācija. Savukārt atbilstoši IT drošības likumā noteiktajam pienākums rūpēties par IKT drošības pārvaldību ir katras iestādes atbildība.MK 2012. gada 19. jūnija noteikumu Nr. 421 „Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības” 7.5. apakšpunktā pieminēts termins „daudzfaktoru autentifikācija”, kas līdz šim nav bijis definēts nevienā normatīvajā aktā. Šis noteikumu projekts definē attiecīgo terminu kā tādu autentifikāciju, kas sastāv no vismaz diviem atribūtiem, kur viens ir atribūts, kuram nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts. Būtiski piebilst, ka noteikumu projekta izpratnē daudzfaktoru autentifikācijas jēdzienam atbilst arī Latvijā izmantotā eParaksta vai eID autentifikācija tajos gadījumos, kad sertifikāts atrodas čipkartē un čipkarte ir aizsargāta ar kodu.Izstrādājot šo noteikumu projektu, izvērtēta arī tā iespējamā ietekme uz MK 2001. gada 30. janvāra noteikumiem Nr. 40 „Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības” (turpmāk – MK noteikumi Nr.40). Konstatēts, ka noteikumi savstarpēji nav pretrunā, jo šis noteikumu projekts ietver arī konkrētas tehniskas prasības, taču MK noteikumi Nr. 40 – tikai vispārējas dokumentu izstrādes prasības (izņemot 5.8. apakšpunktā noteikto – „minimālais paroles garums ir astoņi simboli”). Atbilstoši Oficiālo publikāciju un tiesiskās informācijas likuma 9. panta sestās daļas 2. punktam, ja konstatē pretrunu starp vienāda juridiska spēka vispārējo un speciālo tiesību normu, vispārējo piemēro tiktāl, ciktāl to neierobežo speciālā tiesību norma. |

Anotācijas V sadaļa – projekts šo jomu neskar.

|  |
| --- |
| **VI. Sabiedrības līdzdalība un komunikācijas aktivitātes** |
| 1. | Plānotās sabiedrības līdzdalības un komunikācijas aktivitātes saistībā ar projektu | Projekts sabiedriskajai apspriešanai 2015. gada 1. aprīlī publicēts Aizsardzības ministrijas mājaslapas sadaļā „Sabiedrības līdzdalība”. Uz projekta apspriedi uzaicinātas biedrības „Latvijas atvērto tehnoloģiju asociācija” un „Latvijas Informācijas un komunikācijas tehnoloģijas asociācija”. |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Projekta izstrādē piedalījās attiecīgās jomas speciālisti. Noteikumu projekts ir izskatīts un saskaņots ar CERT.LV Drošības ekspertu grupu, kurā ir komersantu pārstāvji un nevalstisko organizāciju pārstāvji. Uz projekta apspriedi bija ieradušies trīs pārstāvji no divām biedrībām – „Latvijas atvērto tehnoloģiju asociācija” un „Latvijas Informācijas un komunikācijas tehnoloģijas asociācija”.Sabiedriskās apspriešanas laikā saņemti papildu komentāri no biedrības „Latvijas atvērto tehnoloģiju asociācija”. |
| 3. | Sabiedrības līdzdalības rezultāti | CERT.LV Drošības ekspertu grupa konceptuāli atbalsta noteikumu projektu. Visi drošības ekspertu grupas izteiktie komentāri ņemti vērā vai izskatīti starpinstitūciju sanāksmēs.Starpinstitūciju sanāksmēs tika nolemts noraidīt šādus priekšlikumus: 1. CERT.LV Drošības ekspertu grupas priekšlikums papildināt noteikumu projektu ar tiesībām institūcijām neievērot jebkuru no tehniskajām prasībām, ja to ieviešana tehniski nav iespējama, tā vietā nosakot obligātu prasību nodrošināt kompensējošu (alternatīvu) kontroļu esamību. Šis priekšlikums netika pieņemts, jo viens no noteikumu mērķiem ir novērst mantoto (*legacy*) sistēmu izmantošanu, kas vairs neatbilst mūsdienu prasībām. Šobrīd lietošanā ir tādas sistēmas, kas, piemēram, vispār neatbalsta paroļu izmantošanu vai nosaka ļoti nelielu maksimālo paroles garumu, vai arī nenodrošina pietiekamu auditēšanas pierakstu veikšanu. Šādas sistēmas rada pārlieku lielu risku tajās glabātajai informācijai, tāpēc šādas mantotās sistēmas ir apvienojamas, uzlabojamas vai likvidējamas, un to izmantošanu nedrīkst turpināt.
2. Biedrība „Latvijas atvērto tehnoloģiju asociācija” rosināja diskusiju par to, vai konti, kurus institūcijas veido publiskajos sociālajos tīklos, atrodas šo institūciju turējumā vai valdījumā un aicināja noteikt, ka šis MK noteikumu projekts attiecas arī uz šādiem kontiem. Šis priekšlikums neguva atbalstu, jo noteikumi runā par IKT sistēmām un izvirzīt prasības pret publisko sociālo tīklu turētājiem (kas lielākoties ir ārvalstīs reģistrēti komersanti) šobrīd būtu nepraktiski un lieki. Tika panākta vienošanās pie šī jautājuma atgriezties pēc dažiem gadiem, kad institūcijas būs ieviesušas šajā MK noteikumu projektā iekļautās prasības.
3. Biedrība „Latvijas Informācijas un komunikācijas tehnoloģijas asociācija” norādīja, ka noteikumu projektā būtu nepieciešams iekļaut atsauci uz ISO vai LVS standartiem informācijas sistēmu drošības jomā. Priekšlikums netika pieņemts. Projektā sākotnēji bija iestrādātas atsauces uz trim ISO/LVS standartiem, taču starpinstitūciju sanāksmju laikā tika panākta vienošanās šīs atsauces izņemt, pamatojot to ar noteikumu projekta mērķi – padarīt tos pēc iespējas vieglāk īstenojamus un saprotamus, kas izriet no plānotās noteikumu mērķauditorijas (visas valsts un pašvaldību iestādes) un šo institūciju atbildīgo personu zināšanu līmeņa. Argumenti biedrībai tika vēlreiz izskaidroti.

Biedrība „Latvijas atvērto tehnoloģiju asociācija” atbalsta noteikumu projektu, ierosinot veikt astoņas izmaiņas projekta tekstā. Lielākā daļa izmaiņu skar paroļu izveides, maiņas un lietošanas prasības. No iesūtītajām astoņām izmaiņām divas nav ņemtas vērā:1. Ierosinājums aizliegt paroles tekstā iekļaut sistēmas lietotāja konta nosaukumu, sistēmas lietotāja vārdu un uzvārdu nav lietderīgs, jo risks, kas rodas, sistēmas lietotāja parolē iekļaujot sistēmas lietotāja vārdu, uzvārdu vai lietotājvārdu, ir pielīdzināms tam, kas rodas, iekļaujot parolē jebkādus citus vārdnīcas vārdus.
2. Ierosinājums paredzēt, ka noteikumu projekts stājas spēkā pilnā apmērā no 2017. gada 1. janvāra ir pamatots, taču neīstenojams. Aizsardzības ministrija apzinās un atzīst biedrības norādīto risku esamību, ar ko jārēķinās sakarā ar ilgo pārejas periodu. Diemžēl valsts un pašvaldību iestādēm noteikto finansiālo, juridisko un procedurālo ierobežojumu dēļ nav iespējams nodrošināt noteikumos noteikto prasību ieviešanu pilnā apmērā no 2017. gada 1. janvāra.
 |
| 4. | Cita informācija | Projekta izstrādē iesaistīta Valsts reģionālās attīstības aģentūra, CERT.LV, Latvijas Pašvaldību savienība, VAS „Latvijas Valsts radio un televīzijas centrs” un VAS „Elektroniskie sakari”. Projekts elektroniski saskaņots ar Iepirkumu uzraudzības biroju. |

|  |
| --- |
| **VII. Tiesību akta projekta izpildes nodrošināšana un tās ietekme uz institūcijām** |
| 1. | Projekta izpildē iesaistītās institūcijas | Visas valsts un pašvaldību iestādes, 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.Valsts un pašvaldību iestādes funkcijas veiks pieejamo cilvēkresursu ietvaros, jo atbilstoši IT drošības likuma 8. panta otrajai daļai valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā. |
| 3. | Cita informācija | Nav. |

Aizsardzības ministrs R. Bergmanis

Vīza:

valsts sekretārs J. Sārts

09.07.2015. 17:03

3169

K.Solovjovs

67335037; kirils.solovjovs@mod.gov.lv