INFORMATĪVAIS ZIŅOJUMS

Par priekšlikumiem Iekšlietu ministrijas informācijas aprites drošības uzlabošanai

Informatīvajā ziņojumā sniegta informācija par Iekšlietu ministrijas (turpmāk – IeM) un tās padotības iestāžu informācijas un komunikācijas tehnoloģiju (turpmāk - IKT) infrastruktūru un tās aizsardzībai izmantotajiem rīkiem un risinājumiem, raksturota pašreizējā situācija informācijas drošības jomā un sniegti priekšlikumi tās uzlabošanai un atklāto trūkumu novēršanai. Ziņojumā netiek aplūkota Drošības policijai piekritīgā IKT infrastruktūra, kā arī fiziski atdalītā IKT infrastruktūra, kurā tiek apstrādāta informācija dienesta vajadzībām, kā arī valsts noslēpumu saturoša informācija.

Lai risinātu informatīvajā ziņojumā minēto problēmu IeM ir uzsākusi sekojošu uzdevumu plānošanu un īstenošanu:

1. datu pārraides tīkla segmentācija un pieslēgšanās iespēju ierobežošana tam, lai novērstu nevajadzīgu komunikāciju starp iekārtām tīklā un nepieļautu nesankcionētu piekļuvi tīklam;
2. lokālo datu pārraides tīklu centralizēta datu plūsmu analīze ar mērķi identificēt anomālijas;
3. resora iestāžu datortehnikas lietotāju biznesa vajadzību apzināšana un profilēšana tādejādi nosakot ierobežojumus piekļuvei iekštīkla resursiem un lietotņu izmantošanai;
4. jaunas, izolētas datortehnikas pārvaldības infrastruktūras izbūve ņemot vērā apzinātās lietotāju vajadzības un veicot veidojamās infrastruktūras konfigurāciju atbilstoši drošības labajām praksēm t.sk. piesaistot pieredzējušus infrastruktūras drošības konsultantus;
5. vienotas darbstaciju konfigurācijas un drošības pārvaldības rīka ieviešana visā IeM infrastruktūrā ar mērķi unificēt un padarīt caurskatāmus darbstaciju pārvaldības procesus – programmatūras labojumu uzstādīšanu, programmatūras centralizētu izplatīšanu, darbstaciju attālinātu vadību un drošības konfigurāciju.

Būtiskākie jau paveiktie, uzsāktie un vēl veicamie pasākumi iepriekš minēto uzdevumu izpildei ir norādīti informatīvajā ziņojumā, kā arī iekļauti aprēķini par Iekšlietu ministrijai papildu nepieciešamo finansējumu 2018., 2019. un turpmākajiem gadiem sekmīgai uzdevumu īstenošanai. Informatīvajā ziņojumā netiek detalizēti apskatīti organizatoriskie pasākumi, kas jāveic IeM resorā un kam nav nepieciešams papildus finansējums.

Dezklasificēšanas pamatojums: IeM 19.03.2026. vēstule Nr. 1-14/761/26

I.Stafecka
30.04.2026.

1. Pašreizējā situācija un problēmas

1.1. Iekšlietu ministrijas IKT infrastruktūras lietotāji

IeM IKT infrastruktūrā ietilpst aptuveni 8000 datorizētas darba vietas 12 resora iestādēs. IeM IKT infrastruktūras sastāvdaļa ir resora iestāžu pārziņā esošās informācijas sistēmas, kā arī informācijas tehnoloģiju kritiskās infrastruktūras objekti. Netieši IeM IKT infrastruktūru lieto iestādes un personas, kas izmanto resora iestāžu pārziņā esošās informācijas sistēmas un e-pakalpojumus. IeM IKT infrastruktūra tiek izmantota arī IeM iekšējo telefonsakaru nodrošinājumam un IeM radiosakaru sistēmas darbināšanai. IeM IKT infrastruktūru pārvalda un tās darbību nodrošina Iekšlietu ministrijas Informācijas centrs (turpmāk – IeM IC).

1.2. IeM IKT infrastruktūras attīstība

Lai nodrošinātu efektīvāku, vienotu un vienveidīgu IKT tehnoloģiju uzturēšanu un attīstības plānošanu, 2009.gadā tika uzsākti un 2015.gadā pabeigti IKT tehnoloģiju centralizācijas pasākumi[1] IeM resorā.

Līdz tam IeM IKT infrastruktūru uzturēja un attīstīja katra iestāde savu iespēju un izpratnes ietvaros, pielietojot krasi atšķirīgus tehniskos risinājumus, līdz ar to pārvaldība bija decentralizēta, sadrumstalota, bet drošības līmenis – atšķirīgs. Tāpat IeM iestādēm IKT joma ne vienmēr bija prioritāra, kā arī ekonomiskās lejupslīdes iespaidā no 2008. līdz 2012.gadam ievērojamas investīcijas datortīkla attīstībā un datortehnikas atjaunošanā praktiski netika veiktas. Piekļuves līmeņa tīkla infrastruktūra ar autentifikācijas iespējām tika izbūvēta tikai atsevišķās IeM ēkās Rīgā (IeM ēku komplekss Čiekurkalna 1. līnijā, Stabu ielā 89 un daļēji – Bruņinieku ielā 72b) 2008.gadā, kas šobrīd ir morāli novecojusi un programmatūras nestabilās darbības dēļ nenodrošina tīkla līmeņa autentifikāciju (izolāciju).

No 2014.gada finansiālā situācija uzlabojās un laikposmā līdz 2016.gadam IeM resora iestādēs tika nomainīts vairāk nekā 4300 datortehnikas vienību (stacionārie un portatīvie datori). 2017.gadā tika piešķirts[2] papildu finansējums 2 781 000 *euro* apmērā, kas tika izlietots gandrīz 2000 datortehnikas vienību iegādei, pakāpeniski nomainot novecojušo datortehniku, kuru joprojām

[1] 2009.gadā veikta Iekšlietu ministrijas Sakaru centra reorganizācija, pievienojot to IeM IC, pamatojoties uz Ministru kabineta 2009.gada 6.maija rīkojumu Nr.289 "Par Iekšlietu ministrijas Sakaru centra reorganizāciju". Pārņemtas IKT funkcijas un uzdevumi telekomunikāciju un radiosakaru jomā.2010.gadā pārņemtas IeM Informātikas un sakaru nodaļas reorganizētās struktūrvienības funkcijas un uzdevumi saskaņā ar Ministru kabineta 2009.gada 2.jūnija sēdē (prot. Nr. 37 38.§) izskatīto informatīvo ziņojumu „Par iekšlietu sistēmas reorganizāciju", kur tika paredzēti arī pasākumi IKT tehnoloģiju vienotas sistēmas izveidei IeM, IKT resursu optimizācijas un centralizācijas ceļā - IeM sistēmas iestāžu veicamās IKT tehnoloģijas funkcijas līdz 2013. gadam tika pakāpeniski nodotas un IeM IC.

[2] Ministru kabineta 2017. gada 4. oktobra rīkojums Nr.555 "Par apropriācijas pārdali"

darbināja nedrošā Windows XP operētājsistēma, kā arī vadāmo tīkla komutatoru iegādei un tīkla līmeņa piekļuves sistēmas izbūvei. 2018.gadam un turpmākajiem gadiem prioritārā pasākuma "Iekšlietu resora informācijas un komunikācijas tehnoloģiju infrastruktūras drošības uzlabošana" ietvaros apakšpasākumam "Drošas lietotāju darba vides nodrošināšana" piešķirti 384 925 *euro* katru gadu, kas paredzēti datortehnikas iegādei (aptuveni 450 datortehnikas vienību katru gadu). 2018.gadā par papildus piešķirtajiem līdzekļiem uzsākta antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana, kā arī tiek plānota ugunsmūru iegāde un ieviešana apakštīklu aizsardzībai.

1.3. IeM IKT personāls

Iepriekšminētās IKT centralizācijas pasākumi un personāla pārņemšana no IeM iestādēm uz IeM IC funkciju izpildei norisinājās pēc valsts izdevumu samazinājuma kā izejas no globālās recesijas 2008.gadā. Līdz ar to arī izdevumi atlīdzībai, kas tika pārdalīti IeM IC pārņemtajam personālam, atbilda tā brīža samazinājumiem. Laikposmā no 2015. līdz 2017.gadam atlīdzības palielinājumam jauno politikas iniciatīvu un prioritāro pasākumu ietvaros IeM IC piešķirts papildu finansējums 277 420 *euro* apmērā (sakarā ar minimālās mēneša darba algas pieaugumu, uz vienlīdzīgiem principiem balstītas atlīdzības nodrošināšanai), bet 2018.gadam un turpmākajiem gadiem prioritārā pasākuma "Iekšlietu resora informācijas un komunikācijas tehnoloģiju infrastruktūras drošības uzlabošana" ietvaros apakšpasākumam "Datordrošības struktūrvienības izveide" (6 amata vietas) un apakšpasākumam "IKT personāla atlīdzības konkurētspējas uzlabošana" – kopā 793 544 *euro* apmērā, kas paredzēts arī turpmākajiem gadiem.

Tā rezultātā 2018.gadā:

- IeM IC ir izveidota Datordrošības nodaļa, kuras sastāvā iekļauts kvalificēts personāls (6 amata vietas) ar pieredzi darbā ar datordrošības risinājumiem un informācijas sistēmu lietotāju pārvaldībā. Specializētas struktūrvienības izveide nedos tūlītēju rezultātu, taču ļaus fokusēt resursus datordrošības ikdienas jautājumiem, uzlabos kibervides pārskatāmību IeM IKT infrastruktūrā, koncentrēs IKT drošības kompetences, atvieglojot tās pārvaldību un radīs pamatu kompetences attīstībai ilgtermiņā.
- palielināts atalgojums minimālā līmenī (80% apmērā no maksimālā iespējamā mēnešalgas apmēra) piešķirtā finansējuma ietvaros 253 IKT speciālistiem (piemēram, bruto mēnešalga palielināta 71 darbiniekam vidēji no 761 *euro* uz 952 *euro*, 83 darbiniekiem – no 922 *euro* uz 1030 *euro*, vidēji bruto mēnešalgai pieaugot par 136 *euro*).
- pasākuma "Iekšlietu resora informācijas un komunikācijas tehnoloģiju infrastruktūras drošības uzlabošana" ietvaros apakšpasākumam "Personāla apmācība" piešķirts finansējums 19 929 *euro* apmērā katru gadu.

Jo apjomīgāka un sarežģītāka ir pārvaldāmā infrastruktūra, jo augstākas kvalifikācijas un pieredzes darbinieki ir nepieciešami tās uzturēšanai. IeM ir viens no retajiem resoriem, kur IKT pārvaldības centralizācija resora ietvaros jau ir veikta 2009. līdz 2014.gados, tādejādi šobrīd izveidotā infrastruktūra ir salīdzinoši efektīvi centralizēti pārvaldāma, taču tas prasa augstas kvalifikācijas speciālistus ar darba tirgum atbilstošu atalgojumu. IeM IC mēģina piesaistīt augsti kvalificētus speciālistus, kā arī pēc iespējas atbalsta speciālistu kvalifikācijas celšanas pasākumus, taču neskatoties uz papildu finansējuma pieejamību IeM IC personāla atalgojumam, kas vadošajiem speciālistiem atlīdzību regulējošos normatīvajos aktos noteiktā diapazona ietvaros ļauj izmaksāt maksimālo mēnešalgu un piemaksas, joprojām nav iespējams samaksāt atalgojumu, kas būtu konkurētspējīgs ar privātajā sektorā līdzvērtīgiem amatiem piedāvāto atalgojumu. Jāatzīmē, ka IeM IC nav vienīgā valsts pārvaldes iestāde, kas saskaras ar ievērojamu atalgojuma starpību publiskajā un privātajā sektorā, uz to norāda, piemēram, arī SIA "Fontes Vadības konsultācijas" pētījums[3].

1.4. IeM IKT infrastruktūras aizsardzība

IeM IKT drošības politiku nosaka IeM 2011.gada 22.jūnija iekšējie noteikumi nr.24 "IeM un tās padotībā esošo iestāžu IKT resursu drošības pārvaldības pamatprincipi". Šie noteikumi ir novecojuši, tāpēc IeM IKT resursu drošības pārvaldības padome, kuras sastāvā ir gandrīz visu IeM padotības iestāžu drošības pārvaldnieki ir izstrādājusi jaunu iekšējo noteikumu projektu un nodevusi to saskaņošanai. IeM IC kā IeM IKT infrastruktūras darbības nodrošinātājs ir izstrādājis vairākas IeM IC iekšējās procedūras IKT drošības jomā (piem., "Metodiskie norādījumi veicamajām darbībām kiberincidentu gadījumā", IeM IC 2018.gada 4.jūnija; reģ.nr.14-1-5-2/50), tomēr paliek daudzi normatīvie akti un procedūras, kas ir jāaktualizē un jāizstrādā attiecībā uz visu IeM resoru.

IeM iekšējais datu pārraides tīkls sastāv no optiskā datu pārraides tīkla Rīgas pilsētas ietvaros, kas savieno lielākās IeM resora iestāžu ēkas, kas tiek aizsargāts ar centralizēti pārvaldāmiem rīkiem, tīklam ir centralizēti pārvaldāms viens rezervēts savienojuma punkts ar publisko tīklu (Internets). Nevēlamu aktivitāšu atklāšanai un novēršanai IeM iekšējā datu pārraides tīkla iekšienē un tā savienojumos ar citiem tīkliem, t.sk. internetu, jau ilgstoši tiek izmantota virkne ar moderniem šobrīd pasaulē atzītiem un efektīviem drošības risinājumiem:

1. Ielaušanās noteikšanas un novēršanas sistēmas, kas nodrošina no ārpuses veikto uzbrukumu mēģinājumu (incidentu) atklāšanu un bloķēšanu.

[3] http://petijumi.mk.gov.lv/sites/default/files/title_file/salidzinosais_petijums_par_atalgojuma_apmeru.pdf

2. Ugunsmūru un virtuālā privātā tīkla risinājumi starpsavienojumu izveidei un aizsardzībai.
3. Tīkla savienojumu starp IeM datu pārraides tīklu un publisko tīklu kontrolei nodrošina Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (Cert.lv) uzstādītais sensors, kas analizē tīkla robežu šķērsojošo datu plūsmu un informē par iespējamiem informācijas tehnoloģiju drošības incidentiem. Salīdzinājumā ar citiem IeM IC izmantotajiem drošības rīkiem, šī rīka priekšrocība ir iespēja izmantot komerciāli nepieejamus informācijas avotus par ļaunatūru pazīmēm.
4. IeM iekšējā tīkla plūsmu anomāliju analīzes rīks, kas pētot datu plūsmu tīkla līmenī spēj atklāt novirzes no normas.
5. Interneta resursu piekļuves kontroles sistēma (starpniekserveri) - papildus aizsardzībai pret nevēlamu programmu (ļaunatūras) un satura (riska grupā ietilpstošās mājaslapas) nonākšanai IeM datortīklā, kā arī lietotāju piekļuves ierobežošanai nedrošiem interneta resursiem.
6. IeM iekšējam datu pārraides tīklam pieslēgto darba staciju aizsardzībai pret nevēlamu programmu (ļaunatūru) nonākšanai IeM datortīklā tiek izmantota antivīrusa programmatūra.

Neskatoties uz iepriekš minētajiem drošības risinājumiem, jau 2016.gadā tika uzsākts darbs pie papildu drošības rīku iegādes un 2017.gadā:

1. Uzsākta mobilo iekārtu (viedtālruņu un planšetdatoru) drošības risinājuma ieviešana.
2. Ieviests žurnālfailu automatizētas analīzes un kontroles rīks.
3. Uzsākta fizisko tīkla pieslēgumu aizsardzība (802.1x on switch port security).

Piekļuve pie atsevišķiem iepriekš minētajiem jau ieviestajiem drošības rīkiem IeM resora iestāžu par IKT drošību atbildīgajiem darbiniekiem ir nodrošināta tādā apjomā, lai veiktu attiecīgās iestādes izmantotās infrastruktūras lietošanas uzraudzību. Ņemot vērā, ka iestādēs par IKT drošību atbildīgie darbinieki ikdienā nodarbojas ar organizatoriskas un juridiskas dabas jautājumiem IKT drošības jomā, tiem nav atbilstošu tehnisko zināšanu, lai reaģētu uz drošības rīku trauksmes paziņojumiem, veicot tehnisku drošības incidentu izpēti.

Šeit minēto drošības rīku uzraudzību un reakciju uz to trauksmes paziņojumiem līdz 2018.gadam veica par IeM IC IKT infrastruktūras darbību atbildīgie darbinieki paralēli IeM IC IKT infrastruktūras uzturēšanas pienākumiem, kas nebija nodrošināts ne pietiekošā kvalitātē, ne kapacitātē. Šobrīd šo funkciju veic Datordrošības nodaļas personāls.

2018.gadam un turpmākajiem gadiem prioritārā pasākuma "Iekšlietu resora informācijas un komunikācijas tehnoloģiju infrastruktūras drošības uzlabošana" ietvaros apakšpasākumam "Centrālās infrastruktūras aizsardzība"

(programmatūras drošības ielāpu pārvaldības risinājumiem) piešķirts finansējums 139 200 *euro* apmērā katru gadu.

Pēc vairākkārtējām kopējām apspriedēm IeM IC ir sagatavojis "Pasākumu plānu IeM IC uzturētās IKT infrastruktūras drošības uzlabošanai", lai mazinātu IKT drošības riskus, par kuru no Cert.lv ir saņemts atzinums[4], kurā uzsvērta zinoša inženiertehniskā personāla un sakārtota iekšējā normatīvā regulējuma nozīmīgums, kā arī tika norādīts, ka IeM datortīkla infrastruktūras sakārtošanai ir nepieciešama pilnīga Microsoft Active Directory infrastruktūras (turpmāk – AD) pārbūve kontrolēti nošķirot apakštīklus un ierobežojot komunikācijas starp darbstacijām un apakštīkliem. IeM IC sagatavotais "Pasākumu plāns IeM IC uzturētās IKT infrastruktūras drošības uzlabošanai" tika precizēts atbilstoši Cert.lv atzinumam un jau šobrīd tiek īstenoti tie pasākumi, kuru īstenošanu IeM IC var nodrošināt tās pamatfunkciju izpildei piešķirtā finansējuma ietvaros (Inženiertehniskā personāla izglītošana; Kiberincidentu reaģēšanas procedūras izstrāde; IeM normatīvās bāzes sakārtošana IKT drošības jomā; Auditācijas pierakstu analīzes rīka ieviešana, lietošana un spēja reaģēt; Darbstacijā darbināmās programmatūras izpildes ierobežošana; Lietotāju datortehnikas parka homogenizācija), savukārt, lai īstenotu pasākumus atbilstoši CERT.LV atzinumam, kuru īstenošanai ir nepieciešams papildfinansējums, ir sagatavots šis informatīvais ziņojums un kārtējā un vidējā termiņa budžeta likumprojekta sagatavošanas procesā tiks virzīts attiecīgs prioritārā pasākuma pieteikums. Kā viens no būtiskākajiem pasākumiem, kura īstenošana ir uzsākta balstoties uz Cert.lv atzinumu ir antivīrusa risinājuma nomaiņa IeM un padotības iestādēs – 2018.gada jūnijā un jūlijā *Kaspersky* pret *Symantec* ir nomainīts jau >50% galaiekārtās (lietotāju darbstacijās).

2016.gadam un turpmākajiem gadiem jauno politikas iniciatīvu ietvaros piešķirts finansējums 132 000 *euro* apmērā katru gadu datortīkla aizsardzības sistēmas modernizēšanai, pretielaušanās sistēmas paplašināšanai un programmatūras ievainojamības automātiskai atklāšanai.

2018.gadam un turpmākajiem gadiem prioritārā pasākuma "Iekšlietu resora informācijas un komunikācijas tehnoloģiju infrastruktūras drošības uzlabošana" apakšpasākumam "Datu pārraides infrastruktūras aizsardzība" (vadāmu tīkla komutatoru iegādei un tīkla līmeņa piekļuves sistēmas izbūvei, ugunsmūru ieviešanai apakštīklu savstarpējai aizsardzībai ietvaros piešķirts finansējums 162 404 *euro* apmērā katru gadu.

[4] 15.05.2018. CERT.LV vēstule Nr. 5-1/15

2. Veicamie pasākumi IKT drošības uzlabošanas turpināšanai

2.1. Iestādes darbības organizācijas pārskatīšana un atbilstošas kvalifikācijas personāla nodarbināšana

Rīcības izvēle, lai nodrošinātu iestādes funkciju un uzdevumu izpildi, ir iestādes personāla politikas pilnveide. Iestādes darbības organizācijai ir jāatbilst pārvaldītajām tehnoloģijām un cilvēkresursiem, kas pārvalda šīs tehnoloģijas. Personālsastāvam ir jāpiemīt tām prasmēm, zināšanām un spējām, kādas nepieciešamas, lai pārvaldītu, uzraudzītu un attīstītu jau esošās modernās un nākotnes IKT tehnoloģijas. To prasa ne tikai datos balstīta ekonomika, bet arī iekšējā drošība kā funkcija, kas vairs nav tikai fiziskā, bet ietver daudzus mūsdienu tehnoloģiju elementus (droša, centralizēti valdāma koplietošanas datu centru infrastruktūra un datu pārraides tīklu infrastruktūra, valsts informācijas sistēmu koplietošanas platforma, integrētas informācijas apmaiņas platformas kā noziedzības novēršanas un apkarošanas IKT palīglīdzekļi, u.t.l.).

IeM IC uztur vairāk nekā 200 dažādus IKT risinājumus IeM resora iestāžu vajadzībām, tostarp kritiskās infrastruktūras risinājumus, kurus lielākoties valsts drošības apsvērumu dēļ nevar nodot uzturēšanai ārpakalpojumā, tostarp - 28 valsts informācijas sistēmas (pārziņi – PMLP, VP, VRS un IeM IC), operatīvo radiosakaru sistēmu, IeM piekritīgos ārkārtas telefona numurus 112 un 110. Līdz ar aktuālo ES finansēto projektu realizāciju, IeM IC plāno nodrošināt atsevišķu IKT risinājumu uzturēšanu ne tikai IeM resoram, bet arī citām valsts pārvaldes iestādēm ārpus IeM resora.

Ar katru IKT risinājumi tiek pozicionēti kā viens no efektīvākajiem instrumentiem valsts pārvaldes iestāžu pamatdarbības procesu sakārtošanai un to efektīvākai pārvaldībai, taču bez kvalitatīvas un efektīvas IKT sfēras darbības, ir augsts risks nenodrošināt pamata IKT risinājumu darbību ieslīgstot stagnācijā, tādejādi var ciest atbilstošo tiešās valsts pārvaldes funkciju efektīva darbība. Lai izvairītos no šāda scenārija, IeM IC kā vadošajai IeM resora iestādei IKT jomā, jāpārorientē personālsastāvs no novecojušā modeļa, kas asociējas ar informācijas ievadi, apstrādi un vienkāršu datoru iegādi, uz inovatīvu iestādi, kuras personāls pārzin un ir spējīgs piegādāt efektīvi organizētus un kvalitatīvus IKT pakalpojumus. Šādas izmaiņas iespējamas tikai un vienīgi piesaistot kvalificētu un augsti motivētu personālu, tāpēc IeM IC kā pirmie soļi šajā virzienā ir esošo darbinieku amata pienākumu pārskatīšana pakārtojot tos aktuālajiem iestādes darbības virzieniem IKT jomā, tostarp paredzot:

1. atteikšanos no datu ievades operatoru , informācijas sistēminženiera, statistiķu, vecāko referentu amatiem, kas vēsturiski saglabājušies iestādē, jo šobrīd datu ievade, attīstoties valsts informācijas sistēmu funkcionalitātei, notiek uz vietas iestādēs un statistikas aprēķinu metodes ir ievērojami automatizētās, bet IeM IC loma kā datu apstrādes operatoram būtiski mazinājusies, tādejādi ir nepieciešami augsti

kvalificēti sistēmu analītiķi un sistēmu arhitekti, kas aizvietojot datu ievades operatorus spētu kvalitatīvi noskaidrot, aprakstīt un definēt izstrādātājiem informāciju sistēmu funkcionālās (kas sistēmai jādara, t.sk. piemērotākās datu automatizētas apstrādes metodes) un nefunkcionālās (veiktspējas, drošības u.c.) prasības, kā arī koordinēt un pārbaudīt programmēšanas darbus un rezultātus, piedalīties sistēmas testēšanā, uzraudzīt to izstrādi un ieviešanu. Tādējādi tiks nodrošināta IeM IC pārziņā esošo un tuvākajā nākotnē plānoto valsts informācijas sistēmu efektīvāka pārvaldība un attīstība.

Vēršam uzmanību, ka IeM IC ir Iekšlietu resora vadošā IKT jomas iestāde, kuras pārziņā ir liela daļa Iekšlietu vajadzībām izmantojamo valsts informācijas sistēmu, turklāt ir acīmredzama tendence IeM IC uzturamajā integrētajā informācijas sistēmu tehnoloģiskajā platformā integrēt un IeM IC pārziņā un uzturēšanā nodot papildu valsts informācijas sistēmas, kā piemēram:

- Robežsardzes elektroniskā informācijas sistēma (REIS);
- Robežapsardzības informācijas sistēma (RAIS);
- Vienotā 112 ārkārtas palīdzības izsaukumu apstrādes sistēma (112);
- Nacionālā kriminālās izlūkošanas modeļa IKT risinājuma daļas (NKIM).

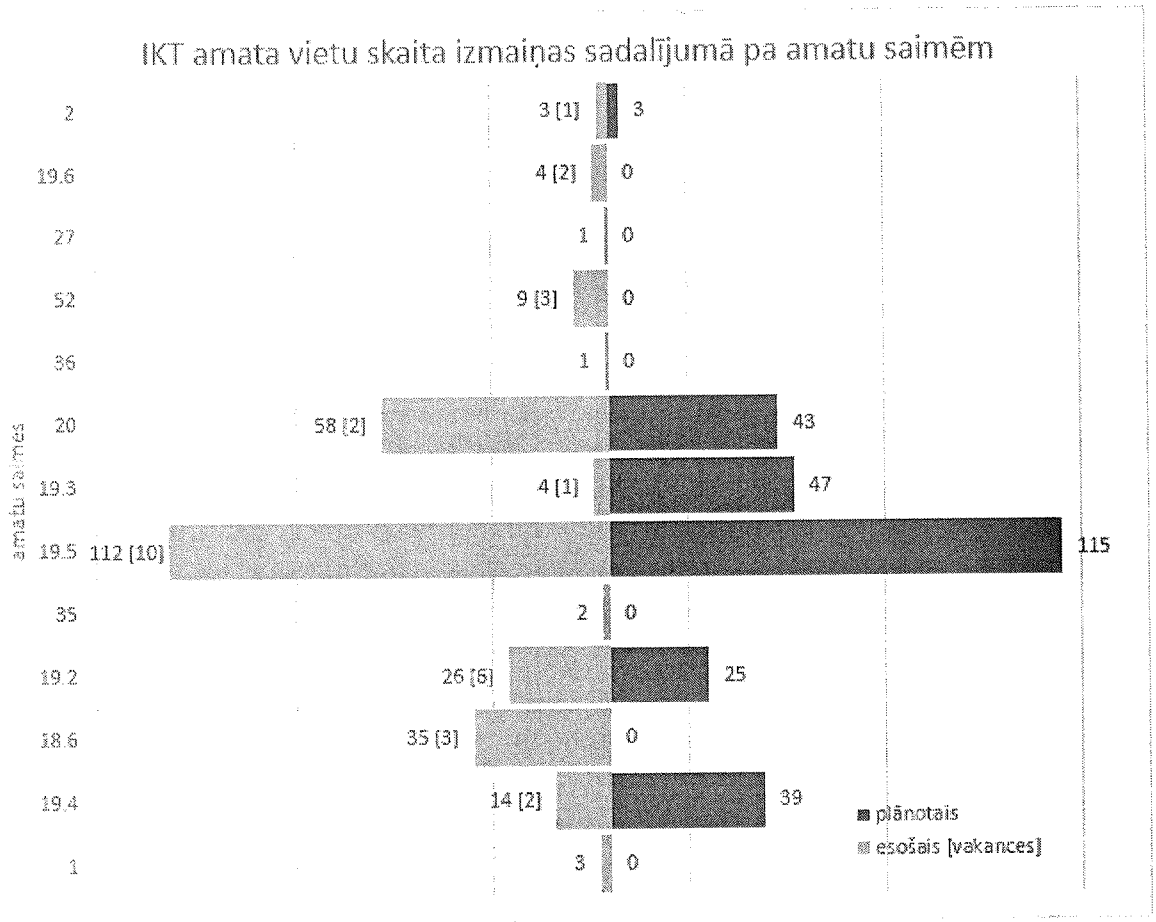
Diemžēl nedz IeM IC, nedz citās IeM iestādēs strauji pieaugot automatizētu informācijas apstrādes sistēmu lomai, nav pietiekošā kvalitātē izdalīti sistēmanalītiķu amati. Sistēmanalītiķiem ir viena no vadošajām lomām faktiski jebkurā IT projektā, jo tieši šie darbinieki pēta biznesa procesus un gadījumā, ja prasības sistēmai ir nepilnīgi noskaidrotas vai izprastas nepareizi, tad neskatoties uz dārgiem izstrādes līgumiem un pieejamu modernu infrastruktūru, projekta gaitā netiks realizēta lietotājiem atbilstoša IT risinājuma izstrāde. Vēsturiski ar sistēmanalīzi un bizsnesa procesu aprakstu sagatavošanu nodarbojušies IeM dienestā esošie darbinieki, kuru primārā kvalifikācija bija atbilstoša dienestam (piemēram, Valsts policijas vai Valsts robežsardzes), taču pieaugot informācijas sistēmu sarežģītībai un nozīmībai ar sistēmanalīzi jānodarbojas augsti kvalificētiem darbiniekiem tieši šajā jomā, pretējā gadījumā laika gaitā var būtiski pasliktināties projektējamo sistēmu kvalitāte, līdz ar to arī valsts pārvaldes iestāžu funkciju izpildes efektivitāte.

2. tehniķus, kas centralizācijas rezultātā tika pārņemti no citām IeM iestādēm un iepriekš veica standarta inženiertehnisko problēmu risināšanu, elektronisko sakaru tīklu apkopi un iekārtu uzturēšanu, tikai savas struktūrvienības ietvaros, ievērojami mazākos apjomos, neizmantojot centralizētus risinājumus, aizvietot ar IT speciālistiem, kas realizē centralizēti vadāmu un sarežģītu datorsistēmu, operētājsistēmu un lietojumu (programmatūras) pakešu ar lielu lietotāju skaitu

administrēšanu, vadīšanu un kontrolēšanu, programmēšanu, datorsistēmu un datortīklu administrēšanu, telekomunikāciju jomas inženiertehnisko darbu veikšanu kopumā visa resora vajadzībām (ļoti lielām iestādēm).

Tehniskā personāla pieredzei, kvalifikācijai, personāla novērtējumam un viņu spējai strādāt ar sarežģītiem centralizētas iekārtu un tīklu pārvaldības risinājumiem, ar kuru palīdzību iespējams panākt augstu konfigurācijas standartizāciju un tās kontroli, ir milzīga loma informācijas un IKT resursu drošībā. Pirms IKT jomas centralizācijas tehniskais personāls bija dažādi kvalificēts, tika nodarbināts dažādās amatu saimēs un līmeņos un ar tādiem pašiem amatiem tehniskie darbinieki tika nodoti IeM IC. Minētie darbinieki jau vairākus gadus (kopš 2014. gada) strādājot IeM IC ietvaros ir bijuši spiesti pieņemt kopējās IKT risinājumu un sistēmu pārvaldības tendences IeM resorā, tika instruēti un iespēju robežās apmācīti izmantot vienveidīgus centralizēti vadāmus un efektīvus rīkus IKT resursu pārvaldībā. Strauji attīstoties IKT risinājumiem, pieaugot valsts informācijas sistēmu kapacitātei un prasībām pret to drošību un pieejamību, tehniķu veicamie pienākumi ir palikuši sarežģītāki tāpēc ir pielāgojami ari to ieņemamo amatu saimes un līmeņi.

Kopumā personāla politikas izmaiņas vērstas uz to, lai pakāpeniski salāgotu notikušās izmaiņas (veikta IeM IKT resursu centralizācija, palielinājies apkalpojamo gala iekārtu un to lietotāju skaits, ieviestas komplicētas IKT sistēmas, pakāpeniski tiek uzsākta ārpus IeM resora esošu iestāžu IKT sistēmu uzturēšana, pastāvīgs kiberdraudu pieaugums) ar pieaugušajām prasībām pret personālu. Plānots, ka lielākā daļa IKT personāla uzlabojot savu kvalifikāciju varēs pildīt paaugstinātās amata prasības. Plānotās amatu saimju izmaiņas attēlotas zemāk esošajā ilustrācijā.



IKT personāla politikas izmaiņu rezultātā IeM IC tiks samazināta amata saimju un līmeņu dažādība no 28 uz 14, tādejādi gan vienkāršojot personāla pārvaldību, gan netieši veicinot personāla izaugsmi, jo līdzīgus uzdevumus veicošajam IKT personālam atalgojums būs atkarīgs no novērtējuma par paveikto.

Veicot norādītās IKT personāla politikas izmaiņas IeM IC atteiksies no mazkvalificētu IKT uzdevumu veikšanas piesaistot jaunu kvalificētu personālu, vai paaugstinot esošā personāla kvalifikāciju, tādejādi pilnvērtīgi nodrošinot komplicētu IKT risinājumu efektīvu darbību un aizsardzību no kiberapdraudējumiem.

2.2. Konkurētspējīga atalgojuma nodrošināšana IKT personālam

IKT infrastruktūras drošības pamatā ir ne tikai šajā informatīvajā ziņojumā minētie mūsdienīgie IKT drošības risinājumi, bet arī atbilstošas kvalifikācijas personāls ("cilvēciskais faktors"), kas vislielākā mērā ietekmē drošības risinājumu pārvaldību un infrastruktūras drošību kopumā. Arī Cert.lv, iesaistoties IeM IKT infrastruktūras drošības incidenta izpētē, ir atzinis, ka, neskatoties uz modernu IKT drošības risinājumu pielietošanu IeM infrastruktūrā, ir nepietiekoša to uzraudzība, nepietiekoša to pielietošana

drošības incidentu noteikšanā, praktiski netiek veikta potenciālo drošības incidentu izmeklēšana, kas ir tiešs rezultāts nespējai valsts pārvaldē piesaistīt kvalificētu IKT personālu, kas esošā atalgojuma sistēmā praktiski nav iespējams.

Salīdzinošais privātā tirgus segmenta pētījums par atalgojumu apmēriem identificē, ka IT sektors ir viens no atalgojuma ziņā straujāk pieaugošākajiem sektoriem, kur pieaugums atlīdzībai ir vismaz 4,1% apmērā gadā. Tikmēr uz valsts sektorā strādājošajiem šīs atlīdzības pieauguma izmaiņas netiek attiecinātas.

Lai apmierinātu vajadzības personāla vadīšanas funkcijas izpildei iestādē, jāveic atlīdzības izmaiņas. 2017.gada dati atspoguļo, ka lielā uzņēmumā privātajā sektorā (vairāk kā 250 darbinieku), kāds ir arī IeM IC, nodarbinātie saņem ievērojami lielāku atalgojumu nekā darbinieki IeM IC pat 2018.gadā (1.tabula). Ņemot vērā izmaiņu procentuālo ikgadējo algu pieaugumu, atšķirības atlīdzības apjomā būs tikai pieaugošas.

1.tabula

IT specialitātes mēnešalgas salīdzinājums privātajā 2017.gadā un Iekšlietu ministrijas Informācijas centrā 2018.gadā [5]

Amats/Rādītājs	Vidējais atalgojums* mēnesī **privātajā sektorā** (darbinieki >250) 2017.gadā	Vidējais atalgojums* mēnesī **IeM IC** (darbinieki >250) 2018.gadā	Starpība pret privāto sektoru, *euro*	Starpība pret privāto sektoru, %
IT vadītājs	2 000	1 045	-955	**-47,75%** ↓
IT speciālists	1 250	884	-366	**-29,28%** ↓
Lietotāju atbalsta speciālists	910	643	-267	**-29,34%** ↓
Programmētājs (1-5 gadu pieredze)	1 600	943	-657	**-41,06%** ↓
Programmētājs (5+ gadu pieredze)	2 500	1 312	-1 188	**-47,52%** ↓
Sistēmu analītiķis	1 380	683	-697	**-50,51%** ↓
Sistēmu arhitekts	2 600	1205	-1 395	**-53,65%** ↓
IT projektu vadītājs	2 000	763	-1 237	**-61,85%** ↓
IT speciālists	1 250	763	-487	**-38,96%** ↓
Sistēmu administrators	1 320	763	-557	**-42,20%** ↓

*Pēc nodokļu nomaksas (neto).

Ņemot vērā to, ka publiskajā sektorā nav iespējams piedāvāt papildus labumus (transportlīdzekļus un mobilos tālruņus personīgām vajadzībām, veselības apdrošināšanu ar papildus labumiem, pensijas uzkrājumus, atlaižu programmas, papildus brīvdienas slimības laikā, bezmaksas ēdināšanu,

[5] Interneta personāla atlases uzņēmuma *CV-Online Latvia* 2018.gada Latvijas algu un atlīdzību pētījums. Pieejams:https://www.cv.lv/pages/algas2018/realplain?utm_source=m.tvnet.lv&utm_medium=banner&utm_campaign=Algas2018&utm_content=320x320, sk. Informācijas tehnoloģijas.

paplašinātu pabalstu loku tml.), jo to neparedz normatīvie akti, atlīdzības apmērs ir būtisks priekšnosacījums visas motivācijas sistēmas uzturēšanai iestādei.

IKT sistēmu komplicētības pieauguma un ārējo kiberapdraudējuma apstākļos strauji aug kvalificēta IT personāla nepieciešamība un tā zināšanu saglabāšanas nozīmē, tāpēc IeM IC turpmāko funkciju un uzdevumu izpildei ir nepieciešams tuvināt atlīdzību IT specialitātē strādājošajiem privātajā sektorā, lai motivētu darbiniekus. Būtu nepieciešams atbilstoši atalgot par paveikto, jo jebkurš darbs ietver līdzsvara elementu – līdzsvaro ieguldītās pūles, prasmes, zināšanas un spējas, ar to, ko darbinieks vēlas saņemt. Ja atlīdzība nešķiet taisnīga, tā demotivē, un darbinieki iegulda mazāk pūļu sasniedzamajā rezultātā. Alga ir galvenais stimuls, tādēļ ļoti svarīgs ir atbilstošs atalgojums, lai noturētu prasmīgus un zinošus speciālistus no to pāriešanas uz privāto sektoru. Atsaucoties uz SIA "Fontes Vadības konsultācijas" pētījuma datiem, ir norādīta vispārēja informācija par to, ka 2017.gadā ir straujākais atalgojuma kāpums pēdējo astoņu gadu laikā – mēneša pamatalgai – 6,3%. Izvirzītais mērķis valsts pārvaldē nodarbināto mēnešalgu tuvināt 80% no līdzīgā amatā nodarbināto vidējām mēnešalgām privātajā sektorā, noteikts Koncepcijā par valsts sektorā nodarbināto vienoto darba samaksas sistēmu.

SIA "Fontes Vadības konsultācijas" pētījumā[6] ir norādīts, ka kritiski svarīgi amati ir arī IT amati, kuri tāpat kā pieredzējuši vadītāji, ir amati, kurus valsts pārvaldē novērtē viszemāk, salīdzinot ar privāto sektoru, kas nozīmē, ka tieši šo amatu algu atšķirības starp valsts pārvaldes un privātā sektora darbiniekiem ir vislielākās. Turpat pētījumā ir norādīts, ka konkrēti šie darbinieki ir tie, kurus darba devējs privātajā sektorā atzīst par visgrūtāk piesaistāmajiem, noalgojamiem un noturamiem. Pētījumā ir secināts, ka, neskatoties uz to, ka atalgojums nav vienīgais darbinieku motivējošais faktors, tomēr pie tik lielas atalgojuma starpības, kāda tā šobrīd ir starp privāto sektoru un valsts pārvaldi, pastāv darbinieku aizplūšanas risks un grūtības piesaistīt jaunus darbiniekus.

IeM IC no 322 amata vietām ir liels īpatsvars amatu, kuru amata pienākumi saistīti ar inženiertehnisko darbu veikšanu (86 amati jeb 26,7% no kopējā amatu skaita), informācijas tehnoloģijām (140 amati jeb 43,5% no kopējā amatu skaita), kā arī IKT politikas attīstības un veicināšanas jautājumiem (kopā 96 amati jeb 29,8% no kopējā amatu skaita).

Pēdējo piecu gadu laikā darba tiesiskās attiecības ar IeM IC ir izbeiguši 66 darbinieki (20,8% no kopējā amatu skaita un 29,2% no IKT jomas amatu skaita). 2018.gada vidū IeM IC ir 30 vakanti IKT amati.

Aizpildot vakantās amatu vietas tiks mazināta pārējo darbinieku pārslodze/spriedze, uzlabosies darba vide un būs iespējams efektīvāk pārvaldīt IKT infrastruktūru, plānot tās attīstību un uzraudzīt tās drošu darbību.

Iestādes kapacitātes stiprināšana ir viens no būtiskākajiem iestādes

[6] http://petijumi.mk.gov.lv/sites/default/files/title_file/salidzinosais_petijums_par_atalgojuma_apmeru.pdf

darbības kvalitātes elementiem. Savukārt, iestādes nodarbināto algu palielināšana sekmēs darbinieku motivāciju un kompetenci. Turpretī šobrīd ir izveidojusies situācija, ka zema atalgojuma dēļ iestādei ir problemātiski nodrošināt kompetentu darbinieku piesaisti un noturēšanu. Tādēļ ir nepieciešams atalgojuma fonda palielinājums, lai nodrošinātu iestādei noteikto funkciju kvalitatīvu izpildi, konkurētspējīgu darbinieku atalgojumu, novērstu personāla mainību un stiprinātu esošos cilvēkresursus, kā arī piesaistītu jaunus kvalificētus speciālistus.

Vēršam uzmanību uz to, ka konkurence starp privāto un publisko sektoru tikai pieaugs, jo nodarbināto skaits IKT sektorā ir ne vairāk kā 2,02% no visu kopējo nodarbināto skaita Latvijā (Certus, 2017) un tas nozīmē, ka cilvēkkapitāls ar nepieciešamajām prasmēm, lai īstenotu digitālos risinājumus, kļūs aizvien ierobežotāks. Bez tam, 45% no tiem jau ir nodarbināti tikai attiecībā uz eksportu, līdz ar to par atlikušajiem 55% no IKT sektorā nodarbinātajiem iekšzemes apgrozījumā publiskajam sektoram ir sīvi jākonkurē ar privāto sektoru. IeM IC nodarbinātajiem IKT jomas speciālistiem ir virkne ierobežojošu faktoru (piemēram, speciālas atļaujas pieejai valsts noslēpumam saņemšana, kas nepieciešama lai strādātu ar valsts kritiskās infrastruktūras objektiem, valsts nozīmes informācijas sistēmām), kas vēl vairāk ierobežo atlikušo IKT jomas speciālistu izvēles iespējas.

IKT jomas speciālistu atalgojuma jautājumi ir izaicinājums daudzās valsts pārvaldes iestādēs, tāpēc ņemot vērā IeM IC uzturamo IKT risinājumu komplicētības pieaugumu, turpmākā IeM IKT personāla politika attīstāma ne tikai paaugstinot amata prasības un pārskatot amatu aprakstus, bet arī uzlabojot atlīdzības konkurētspēju, un attiecīgi tiem atbilstošās mēnešalgu grupas. Iepriekšējā punktā aprakstītās personāla politikas izmaiņas ļauj pārskatīt arī personāla atalgojumu. Personāla politikas pilnvērtīgai īstenošanai nepieciešamo izdevumu detalizēts aprēķins iekļauts šī ziņojuma 2.pielikumā.

Ņemot vērā pieejamo papildu finansējumu personāla atalgošanai un kvalifikācijas celšanai, ierastajā kārtībā tiks veikta esošo darbinieku novērtēšana attiecīgi vērtējot katra darbinieka personīgo ieguldījumu, pieredzi amata pienākumu izpildē, tā veicamā darba nozīmīgums IeM IC ietvaros un arī darbinieka kvalifikāciju. Nav plānota masveida darbinieku atlaišana, bet ir iespējama darba attiecību pārtraukšana vai rotācija atsevišķiem nepietiekoši vai neatbilstoši kvalificētiem darbiniekiem. Vēršam uzmanību, ka jau ilgstoši IeM IC darbiniekiem veicot ikgadējo personāla novērtēšanu kopējais novērtējums pārsvarā ir "ļoti labi" vai augstāk (piemēram - 2017.gadā 71%), tāpēc kopumā esošo IeM IC darbinieku kvalifikācija lielākajā vairumā gadījumu ņemot vērā jau iegūto pieredzi, būs pietiekoša darba gaitu turpināšanai IeM IC. Nepārprotami lielai daļai darbinieku būs nepieciešama papildu izglītošana, kas saistīta ar konkrētās darbības jomas kvalifikācijas celšanas kursu apmeklēšanu. Līdz ar atalgojuma palielināšanos, pieejamā budžeta ietvaros plānotas arī darbinieku papildu kvalifikācijas celšanas aktivitātes, tādejādi motivējot

apmācītos un pieredzi guvušos speciālistus, saņemot darba tirgum atbilstošu atalgojumu, turpināt darbu IeM IC , nevis pāriet darbā privātajā sektorā.

2.3. IeM iekšējās normatīvās bāzes IKT drošības jomā sakārtošana

IeM iekšējie normatīvie akti IKT drošības jomā ir pārstrādājami atbilstoši aktualitātēm IKT drošības jomā un šajā informatīvajā ziņojumā minētajiem īstenojamajiem pasākumiem, tādejādi IeM un padotības iestādēs ieviešot IKT drošības politiku un sakārtojot ar to saistītās procedūras.

2.4. Datu pārraides tīkla segmentācija

Pasākums ir priekšnosacījums jaunās Microsoft Active Directory infrastruktūras izbūvei, bez kā realizācijas nav iespējama jaunās infrastruktūras izbūve. Sastāv no diviem posmiem:

1. Visu IeM datu pārraides tīkla pieslēgumu punktu t.sk. datu centru aprīkošana ar ugunsmūriem. Kopš 2015.gada, strauji mainoties IKT drošības situācijai, ir pieaudzis gan potenciālo apdraudējumu daudzums, gan uzbrukumu sarežģītība. It īpaši ir mainījušie apdraudējumu vektori, paaugstinot iekšējo resursu aizsardzības nepieciešamību. Pieaugot varbūtībai, ka apdraudējums var rasties iekšējā datortīklā, vairs nepietiek tikai ar Iekšlietu ministrijas datortīkla ārēja perimetra aizsardzību, tāpēc, ņemot vērā, ka šobrīd IeM iekšējais tīkls pieļauj komunikāciju starp pilnīgi jebkuru tīklam pieslēgtu iekārtu, ir jāpastiprina gan iekšējo komunikāciju kontrole, gan jāceļ barjeras apdraudējumu izplatīšanai Iekšlietu ministrijas datortīkla ietvaros, izmantojot daudzlīmeņu aizsardzības pieeju – uzstādot kompleksās ugunsmūru drošības iekārtas.

Jāatzīmē, ka iepriekšējos gados ugunsmūru iegādei tika piešķirts pastāvīgs finansējums 86 902 *euro* apmērā, taču ar šādu finansējuma apjomu ugunsmūra iekārtu iegāde nepieciešamajā apjomā būs iespējama vien 4 gadu laikā, turklāt bez tajos izmantojamās vadības programmatūras ražotāja atbalsta, kas radītu papildu riskus ugunsmūru nepārtrauktas darbības nodrošināšanā. IeM IC esošo cilvēkresursu un to kvalifikācijas ietvaros nav iespēju samērīgā laika periodā uzstādīt minētās iekārtas, jo katra no tām ir atbilstoši jānokonfigurē, jānogādā kādā no IeM iestāžu struktūrvienībām Latvijas teritorijā, jāsaskaņo konfigurācija ar datu pārraides pakalpojumu sniedzēju, jāsaskaņo tīkla dīkstāves laiki ar atbilstošo struktūrvienību, kā rezultātā bieži vien darbi veicami ārpus darba laika. Tāpēc lai līdz 2020.gada vidum visus IeM datu pārraides tīkla punktus aprīkotu ar ugunsmūru iekārtām nepieciešams papildu finansējums to iegādei un uzstādīšanai. Detalizēts aprēķins iekļauts šī ziņojuma 1.pielikuma 1.tabulā.

2. **Piekļuves līmeņa komutatoru nomaiņa** - Neskatoties uz veiktajiem ieguldījumiem drošu piekļuves līmeņa komutatoru iegādē 2017.gadā lielākajiem IeM resora lokālajiem tīkliem Rīgas robežās, jaunās AD infrastruktūras izolācija būs jāveic gandrīz visos IeM iestāžu lokālajos tīklos visā Latvijas teritorijā. Ar

esošajiem lokālo datu pārraides tīklu komutatoriem un esošo lokālo tīklu vadu instalācijas izpildījumu tas nav iespējams, jo IeM iestāžu struktūrvienības ir izvietotas galvenokārt relatīvi vecās ēkās, kuru būvniecības stadijā nav projektēti pilnvērtīgi lokālie komunikāciju tīkli, taču IT tehnoloģijām strauji attīstoties no 2000–šo gadu sākuma, lokālie komunikāciju tīkli tika būvēti haotiski, līdzekļi to instalācijā tika ieguldīti tikai akūtas nepieciešamības gadījumā, rezultātā nesakārtota tīklu instalācija ir 77 objektos. Tikai pēc lokālo tīklu instalācijas sakārtošanas iespējama atbilstošu komutatoru nomiņa. Komutatoru nomiņa paredzētu gan iespējas izolēt kompromitēto infrastruktūras daļu no jaunās, gan automatizēt gala iekārtu drošas pieslēgšanas darbus, gan nodrošināt drošus autentifikācijas līdzekļus, lai lokālajiem tīkliem nevarētu pieslēgties patvaļīgi. Komutatoru iegādei nepieciešama papildu finansējums. Šāda apjoma tehnikas nomaiņai un kvalitatīvai, nesasteigtai darbu norisei nepieciešama atbilstoša ārpakalpojuma piesaiste. Detalizēts aprēķins iekļauts šī ziņojuma 1.pielikuma 1.tabulā.

2.5. Microsoft Active Directory jaunas infrastruktūras projektēšana un datortehnikas migrācija

Pirms jaunas AD infrastruktūras ieviešanas nepieciešama tās drošības arhitektūras izstrāde iesaistot arī kvalificētus ārējos ekspertus – konsultantus. Uzsākot migrāciju uz nedrošu un nepietiekoši aizsargātu vai neatbilstoši uzprojektētu AD infrastruktūru, pastāv ļoti augsti riski, ka tā var tikt atkārtoti kompromitēta. Projektēšanas gaitā jāparedz visu jau ieviesto drošības risinājumu implementācija jaunajā AD infrastruktūrā. Atbilstošas kvalifikācijas ārpakalpojuma piesaistei nepieciešams papildu finansējums. Detalizēts aprēķins iekļauts šī ziņojuma 1.pielikuma 1.tabulā. Galvenie veicamie uzdevumi:

1. AD infrastruktūras projekta un drošas konfigurācijas izstrāde tieši IeM infrastruktūrai, drošas migrācijas ieteikumu izstrāde iekļaujot datortehnikas, AD integrēto risinājumu, lietotāju datu, lietotāju e-pastu, koplietošanas resursu, u.c. informācijas resursu migrācijas scenārijus;
2. lietotāju profilēšana pēc izmantojamajiem IKT risinājumiem, lietotāju normālas uzvedības datu pārraides tīklā definēšana (ugunsmūra politikas), lietotāju normālas uzvedības datortehnikas lietošanā definēšana (auditācijas pierakstu analīzes rīka politiku izveide).

IeM datu pārraides tīklam ir pieslēgti un ikdienā aktīvi tiek lietoti 8000 datori, pēc jaunās AD infrastruktūras projektēšanas un atbilstošu sistēmu konfigurācijas būs jānodrošina visas datortehnikas operētājsistēmu pārinstalēšana, lietotāju datu pārnešana un datoru pieslēgšana jaunajai AD infrastruktūrai. Šāda apjoma datoru migrācijai IeM IC darbiniekiem paralēli veicot arī citus šajā ziņojumā aprakstītos pasākumus un ikdienas IKT lietotāju problēmu risināšanu, nav iespējama bez papildu ārpakalpojuma piesaistes.

2.6. E-pasta risinājumu nomaiņa

Viennozīmīgi viena no populārākajām metodēm inficētu datņu vai viltus norāžu iesūtīšanai aizsargātā infrastruktūrā ir e-pasts. Veicot jaunas, izolētas AD infrastruktūras izbūvi ir jānodrošina, ka tā netiktu kompromitēta iesūtot tajā atbilstošus e-pastus, līdz ar ko tajā ir jānodrošina vienots, drošs e-pasta risinājums. Esošie IeM resora vajadzībām izmantotie e-pasta risinājumi ir vairāki, to pārvaldība ir neefektīva - decentralizēta. Pamatā tiek izmantoti bezmaksas atvērtā koda risinājumi, kā arī slēgta koda pārvaldības risinājumi izstrādāti pamatā Āzijas valstu tirgum.

Parasti valsts pārvaldes iestāžu vidū populāras ir Microsoft e-pasta sistēmas, taču globālās recesijas ietvaros 2009.gadā IeM resors finanšu ekonomijas nolūkos bija spiests atteikties no dārgiem korporācijas Microsoft lielapjoma licencēšanas līgumiem, kas ļauj izmantot jaunākos, drošākos un modernākos programmatūras produktus, kā rezultātā migrācija uz IeM resora mērogam atbilstošu komerciālu e-pasta risinājumu nav bijusi iespējama. Esošo e-pasta risinājumu pieslēgšana jaunajai AD infrastruktūrai radītu potenciālus drošības riskus, tāpēc nepieciešama atbilstoša komerciālas e-pasta risinājuma iegāde. Detalizēts aprēķins iekļauts šī ziņojuma 1.pielikuma 1.tabulā.

2.7. Datoram pieslēdzamo datu nesēju kontrole

Viennozīmīgi viena no populārākajām metodēm aizsargātas infrastruktūras inficēšanai, tāpēc jaunas AD infrastruktūras izbūvē šīs ļaunatūras pārnēsāšanas metodes apkarošanai tiks pievērsta pastiprināta uzmanība. Ar esošajiem cilvēkresursiem tiks implementēti atbilstoši rīki, kuru iegādei atbilstošs finansējums jau piešķirts 2018.gadā.

2.8. Sistemātisku IKT risinājumu drošības testu veikšana

Ilgtermiņā pēc jaunas AD infrastruktūras izbūves būtu nepieciešams panākt situāciju, ka regulāri tiek veikti IKT infrastruktūras drošības testi (datordrošības un atbilstības pārbaude, ielaušanās tests un rekomendāciju sagatavošana), lai pārliecinātos par IeM infrastruktūras drošību un noturību pret kiberdraudiem. Primāri tiek plānots veikt drošības testus publiskajā elektronisko sakaru tīklā pieejamajām valsts informācijas sistēmām un kritiskajai IKT infrastruktūrai, kam līdz šim finansējums nebija paredzēts. Provizoriski nepieciešamais finansējums ir 20 000 *euro* katru gadu, sākot ar 2019.gadu. Izmaksas iekļautas šī ziņojuma 1.pielikuma 1.tabulā.

3. Secinājumi

Veiktā IeM IKT resursu centralizācija ļāva unificēt tās pārvaldīšanu, identificēt trūkumus un uzsākt pakāpenisku kontrolējamu drošības līmeņa uzlabošanu, izmantojot centralizēti pārvaldāmus risinājumus.

Saskaņā ar Cert.lv ieteikumiem un papildu piešķirtajam finansējumam jau 2018.gadā tiek realizēti dažādi IeM IKT infrastruktūras drošības uzlabojumi, t.sk. ir mazināta nedrošu datortehnikas operētājsistēmu izmantošana, tomēr iespēju robežās jāturpina aprakstīto drošības pasākumu ieviešana.

Nav pietiekoši cilvēkresursi IKT drošības pārvaldības jomā, ar grūtībām notiek jauna IT personāla piesaiste un esošā IT personāla motivēšana noturēšanai darbā IeM.

Ņemot vērā iepriekš minēto, jāuzsāk jaunas Microsoft Active Directory infrastruktūras izbūve un saistīto drošības pasākumu plānveida ieviešana IeM IKT infrastruktūras drošības uzlabošanai.

Neveicot šajā informatīvajā ziņojumā minētos pasākumus, iespējama tālāka ļaunatūras izplatība IeM datortīklā, tādejādi var paaugstināties IeM un padotības iestāžu informācijas noplūdes un tehnisko resursu nepieejamības riski.

4. Finansēšanas avoti

Lai risinātu šajā ziņojumā norādītās problēmas jau 2018.gadā, Iekšlietu ministrija ierosina veikt finansējuma pārdales:

1) no budžeta apakšprogrammas 40.02 00 00 "Nekustamais īpašums un centralizētais iepirkums" 500 000 *euro*.

2) budžeta apakšprogrammas 02.03.00 "Vienotās sakaru un informācijas sistēmas uzturēšana un vadība" ietvaros starp pasākumiem un izdevumu klasifikācijas kodiem atbilstoši ekonomiskajām kategorijām (turpmāk – EKK).

1. **Finansējuma pārdale no budžeta apakšprogrammas 40.02.00 "Nekustamais īpašums un centralizētais iepirkums" 500 000 *euro*** (detalizēts aprēķins šī ziņojuma 1.pielikuma 1.tabulā).

Likumā "Par valsts budžetu 2018. gadam" pasākumam "Investīciju projektu īstenošanai nepieciešamās publikās un privātās partnerības dokumentācijas sagatavošana" plānots finansējums 750 000 *euro* apmērā. Ņemot vērā Valsts kontroles revīzijas "Iekšlietu nozares nekustamo īpašumu pārvaldīšanas likumība un efektivitāte" konstatējumus, Iekšlietu ministrija ir pieņēmusi lēmumu pārvērtēt gan investīciju programmā iekļaujamos objektus, gan sākotnēji objektos plānotās platības, gan iestāžu izvietojumu. Līdz ar to nav nepieciešams sagatavot privātās partnerības līguma projektu un plānotais finansējums 2018.gadā netiks apgūts. Nodrošinājuma valsts aģentūrai

(budžeta apakšprogramma 40.02.00 "Nekustamais īpašums un centralizētais iepirkums") ir izveidojusies finanšu līdzekļu ekonomija 750 000 *euro* apmērā.

Lai nodrošinātu pieslēguma punktu, tajā skaitā datu centru, aprīkošanu ar ugunsmūriem un piekļuves līmeņa komutatoru nomaiņu, nepieciešams finansējums 500 000 *euro* apmērā.

Ņemot vērā to, ka finansējumu 750 000 *euro* apmērā plānots pārdalīt arī citiem Iekšlietu ministrijai nepieciešamiem pasākumiem, kuri veicami 2018.gadā, Iekšlietu ministrija sagatavos un virzīs atsevišķu Ministru kabineta rīkojuma projektu par apropriācijas pārdali no pasākuma "Investīciju projektu īstenošanai nepieciešamās publikās un privātās partnerības dokumentācijas sagatavošana".

2. **Finansējuma pārdale budžeta apakšprogrammas 02.03.00 "Vienotās sakaru un informācijas sistēmas uzturēšana un vadība" ietvaros** (detalizēts aprēķins šī ziņojuma 1.pielikuma 2., 3. un 4.tabulā).

Iekšlietu ministrijai (Iekšlietu ministrijas Informācijas centram), lai ar datortīkla drošības iekārtām aprīkotu 5 Iekšlietu ministrijas resora iestāžu reģionālās pārvaldes (galvenokārt, Valsts robežsardzes pārvaldes) un 35 reģionālās struktūrvienības (Pilsonības un migrācijas lietu pārvaldes un Valsts robežsardzes struktūrvienības) un nodrošinātu iepriekšējos periodos iegādāto programmproduktu uzturēšanu nepieciešams finansējums 255 755 *euro* apmērā. Nepieciešams iegādāties:

– 11 dažādas veiktspējas datortīkla drošības iekārtu iegāde;

– 170 programmproduktu uzturēšanas iegāde kas nepieciešamas, lai nodrošinātu datordrošības iekārtu pilnvērtīgu darbību;

– 4 informācijas sistēmu programmatūras ievainojamības automātikas atklāšanas licenču uzturēšanas nodrošināšana.

2016. un 2017.gadā IeM IC ieviesa šādus pasākumus informācijas un komunikācijas tehnoloģiju drošības jomā – "Tehnisko resursu auditācijas pierakstu savākšana, integrēšana un analīzes reālajā laikā", "Pārnēsājamo iekārtu centralizēts drošības pārvaldības risinājums", "Informācijas sistēmu programmatūras ievainojamības automātiskas atklāšanas sistēma", kā arī Iekšlietu ministrijas padotībā esošo iestāžu reģionālo struktūrvienību datortīklu aizsardzības sistēmas izveide. Pasākumu ieviešanas rezultātā tika iegādāti un tiek pielietoti trīs IT drošības risinājumi, bet ceturtais atrodas ieviešanas stadijā. Minēto risinājumu provizoriskās iegādes izmaksas tika rēķinātas vēl pirms 2016. gada, taču mūsdienās straujas IKT risinājumu attīstības ietvaros, pa šo laiku ir mainījušies attiecīgo risinājumu ražotāju gan licencēšanas, gan uzturēšanas izmaksas un nosacījumi.

Ņemot vērā budžeta izpildes rādītājus 2018.gadā un pasākumu ieviešanas rezultātus, Iekšlietu ministrijas Informācijas centram (budžeta apakšprogramma 02.03.00 "Vienotās sakaru un informācijas sistēmas

uzturēšana un vadība") ir izveidojusies finanšu līdzekļu ekonomija 255 755 *euro* apmērā šādiem valsts drošības stiprināšanas pasākumiem (turpmāk – neatliekamais pasākums):

– "Pārnēsājamo iekārtu centralizēts drošības pārvaldības risinājums" **4 788** ***euro***. Līdzekļu ekonomija izveidojusies, jo programmatūras jauninājumu un ražotāja tehniskā atbalsta abonēšanas izmaksas ir ievērojami zemākas, nekā 2015.gadā tika prognozētas.

– "Tehnisko resursu auditācijas pierakstu savākšana, integrēšana un analīze reālajā laikā" **250 967** ***euro***. 2016.gadā, pirms tehnisko resursu auditācijas pierakstu savākšanas, integrēšanas un analīzes reālajā laikā programmatūras licenču iegādes, tika veikta visaptveroša potenciālo tehnisko risinājumu testēšana un vairāku pilotprojektu īstenošana. Tā rezultātā ir izdevies iegādāties tādus produktus, kuru licencēšanas un uzturēšanas izmaksas ir ievērojami zemākas par sākotnēji plānotajām.

Lai nodrošinātu finansējuma avotu izdevumu segšanai 2018.gadā, Iekšlietu ministrija ierosina veikt apropriācijas pārdali budžeta apakšprogramma 02.03.00 "Vienotās sakaru un informācijas sistēmas uzturēšana un vadība" ietvaros starp EKK un pasākumiem, samazinot finansējumu neatliekamajiem pasākumiem ("Pārnēsājamo iekārtu centralizēts drošības pārvaldības risinājums", "Tehnisko resursu auditācijas pierakstu savākšana, integrēšana un analīze reālā laikā") 255 755 *euro* apmērā un attiecīgi palielinot finansējumu, lai segtu izdevumus, kas saistīti ar datortīkla drošības iekārtu iegādi un to atbalsta nodrošināšanu; kā arī pārdalot finansējumu starp EKK neatliekamā pasākuma "Informācijas sistēmu programmatūras ievainojamības automātiskas atklāšanas sistēma" ietvaros.

Likuma "Par valsts budžetu 2018.gadam" 30.pants nosaka, ka finanšu ministram ir tiesības budžeta resoram likumā noteiktās apropriācijas ietvaros pārdalīt apropriāciju starp programmām, apakšprogrammām, budžeta izdevumu kodiem atbilstoši ekonomiskajām kategorijām, ievērojot arī nosacījumu (10.punkts), ka nav pieļaujama apropriācijas pārdale citiem mērķiem no neatliekamajiem pasākumiem 2016.-2018.gadam, jaunajām politikas iniciatīvām un citiem prioritārajiem pasākumiem 2017.-2019.gadam un prioritārajiem pasākumiem 2018.-2020.gadam piešķirtā finansējuma.

Savukārt minētā likuma 31.panta 5.punkts nosaka, ka šā likuma 30.panta nosacījumi neattiecas uz apropriācijas pārdali starp programmām, apakšprogrammām un budžeta izdevumu kodiem atbilstoši ekonomiskajām kategorijām budžeta resoram likumā noteiktās apropriācijas ietvaros, ja ir pieņemts Ministru kabineta lēmums un Ministru kabinets ir deleģējis finanšu ministram tiesības veikt apropriācijas pārdali, nepiemērojot šā likuma 30.panta nosacījumus. Šādu apropriācijas pārdali atļauts veikt, ja Saeimas Budžeta un finanšu (nodokļu) komisija piecu darba dienu laikā no attiecīgās informācijas saņemšanas nav iebildusi pret apropriācijas pārdali.

Lai risinātu šajā ziņojumā norādītās problēmas 2019.gadā un turpmākajos gados jautājumu par papildu nepieciešamo finansējumu 2019.gadā **4 649 384** ***euro***, 2020.gadā **4 334 450** ***euro***, 2021.gadā **4 021 980** ***euro*** un 2022.gadā un turpmāk katru gadu **3 376 731** *euro* apmērā (detalizēts aprēķins šī ziņojuma 1.pielikuma 1.tabulā) Iekšlietu ministrijai budžeta apakšprogrammā 02.03.00 "Vienotās sakaru un informācijas sistēmas uzturēšana un vadība", jāizskata Ministru kabinetā kopā ar visu ministriju un citu centrālo valsts iestāžu priekšlikumiem prioritārajiem pasākumiem likumprojekta "Par valsts budžetu 2019.gadam" un likumprojekta "Par vidēja termiņa budžeta ietvaru 2019., 2020. un 2021.gadam" sagatavošanas un izskatīšanas procesā atbilstoši valsts budžeta finansiālajām iespējām.

Iekšlietu ministrs Rihards Kozlovskis

Vīza:
valsts sekretārs Dimitrijs Trofimovs

20.09.2018. 9:03
5962
S.Kanteruks, 67208634
Sergejs.Kanteruks@ic.iem.gov.lv