INFORMATĪVAIS ZIŅOJUMS

Par priekšlikumiem Iekšlietu ministrijas informācijas aprites drošības uzlabošanai

Informatīvajā ziņojumā sniegta informācija par Iekšlietu ministrijas 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.

1. PAŠREIZĒJĀ SITUĀCIJA UN PROBLĒMAS

1.1. Iekšlietu ministrijas IKT infrastruktūras lietotāji

Iekšlietu ministrijas IKT infrastruktūrā ietilpst aptuveni 8100 datorizētas darba vietas šādās iestādēs:

- Iekšlietu ministrija (IeM),
- Valsts policija (VP),
- Valsts robežsardze (VRS),
- Valsts ugunsdzēsības un glābšanas dienests (VUGD),
- Pilsonības un migrācijas lietu pārvalde (PMLP),
- Iekšējās drošības birojs (IDB),
- Nodrošinājuma valsts aģentūra (NVA),
- Iekšlietu ministrijas Informācijas centrs (IeM IC),
- Iekšlietu ministrijas veselības un sporta centrs (IeM VSC),
- Valsts policijas koledža (VPK),
- Ugunsdrošības un civilās aizsardzības koledža (UCAK),
- Valsts robežsardzes koledža
- VSIA "Iekšlietu ministrijas poliklīnika".

IeM IKT infrastruktūras sastāvdaļa ir iepriekš minēto iestāžu pārziņā esošās informācijas sistēmas, kā arī informācijas tehnoloģiju kritiskās infrastruktūras objekti. Netieši IeM IKT infrastruktūru lieto iestādes un personas, kas izmanto iepriekš minēto 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 IeM IC. Līdz 2013.gadam liela daļa IeM IKT infrastruktūras (t.sk. lietotāju darba vides nodrošināšana) bija pašu iestāžu uzdevums.

Dealklasificēšanas pamatojums: IeM 24.07.2023. vēstule Nr. 1-14/1817
I.Stafecka 09.10.2024.

1.2. IeM IKT infrastruktūras attīstība

2012.-2014.gadā tika veikta IeM IKT infrastruktūras centralizācija IeM resorā, t.i., IeM IC pārņēma IeM iestāžu IKT infrastruktūras pārvaldību, personālu un pieejamo finansējumu. Līdz tam laikam IeM IKT infrastruktūru uzturēja un attīstīja katra iestāde savu iespēju un izpratnes ietvaros, kas noveda pie krasi atšķirīgu tehnisko risinājumu pielietošanas, to decentralizētas pārvaldības, sadrumstalotības un atšķirīga drošības līmeņa.

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. No 2014.-2016.gadam IeM iestādēs tika nomainīts nedaudz vairāk nekā 4300 datortehnikas vienību (stacionārie un portatīvie datori), taču joprojām IeM infrastruktūrā ir sastopami arī 8 gadus veci datori, aptuveni 1000 no tiem darbojas, izmantojot novecojušo Windows XP operētājsistēmu. Piekļuves līmeņa tīkla infrastruktūra ar autentifikācijas iespējām tika izbūvēta tikai dažās 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).

1.3. IeM IKT personāls

Neskatoties uz veiktajiem pasākumiem IKT personāla darba apstākļu uzlabošanai, galvenais personālu motivējošais elements tomēr ir mēnešalga. Pašreizējais mēnešalgas apmērs nav motivējošs, līdz ar to nav izdevies novērst kvalificēta IKT personāla aizplūšanu.

Lai gan augstākā līmeņa IKT speciālistu, tostarp attiecīgo struktūrvienību IKT vadītāju, atalgojums pēdējo gadu laikā tuvinās privātajā sektorā strādājošo algām, tomēr joprojām ir ievērojamas atšķirības – vidējais atalgojums IKT pakalpojumu jomā 2017.gada pirmajā ceturksnī bija 1331 EUR (bruto) (Centrālā statistikas pārvalde, 2017[1]), bet IeM IC vidējais atalgojuma līmenis ir 1100 EUR (bruto) (IeM IC, 2017.gada pirmajā pusgadā).

Tāpat arī Valsts kancelejas pasūtītajā pētījumā par 2016.gadu ir secināts, ka tieši 19. un 20.amatu saimē ir vislielākās novirzes **mēneša pamatalgā** – attiecīgi -57% (**informācijas tehnoloģijas**) un -52% (**inženiertehniskie darbi**) no privātā sektora atalgojuma (Valsts kanceleja, 2016[2]). Kopumā valsts sektorā strādājošiem ir arī mazākas papildus sociālās garantijas – veselības apdrošināšanas polišu servisa līmenis nesniedz visus iespējamos piedāvājumus,

[1] Centrālā statistikas pārvalde. 2017. http://www.csb.gov.lv/statistikas-temas/darbaspeka-izmaksas-galvenie-raditaji-30319.html.

[2] SIA "Fontes vadības konsultācijas". 2016. "Salīdzinošais pētījums par atalgojuma apmēru". http://petijumi.mk.gov.lv/sites/default/files/title_file/salidzinosais_petijums_par_atalgojuma_apmeru.pdf.

kā arī netiek veiktas valsts kā darba devēja iemaksas 3.līmeņa pensiju fondos.[3] Pārējais nodrošinājums sociālo garantiju jomā valsts un privātajā sektorā ir samērā līdzīgs, tāpēc izšķiroši ir nodrošināt pamata mēnešalgu atalgojuma pieaugumu, lai izlīdzinātu savstarpējo konkurētspēju par kvalificētiem IKT speciālistiem.

Jāatzīmē, ka atšķirīgajam atalgojuma līmenim nav rodams pamatojums attiecībā uz darba apjomu un izpildes kvalitāti, jo:

1) publiskajā sektorā strādājošo atalgojums ir zemāks, bet ir salīdzinoši prasīga darba vide – drošības risku un incidentu novēršana pašreizējos ģeopolitiskajos apstākļos, valsts kritiskās infrastruktūras uzturēšana un nepārtrauktas valsts informācijas sistēmu infrastruktūras un datu apmaiņas procedūru izmaiņas, ņemot vērā normatīvo aktu grozījumu apjomus;

2) lai gan darba laiks atšķirībā no privātā sektora ir vairāk prognozējams, tomēr praksē reti iekļaujas noteiktajās darba stundās, jo kritiski svarīgu valsts informācijas sistēmu uzlabošanas darbi netiek veikti darba laikā, jo tās ir jālieto citām valsts iestādēm. Sevišķi, paaugstinātu drošības incidentu risku apstākļos, notiek gan infrastruktūras, gan valsts informācijas sistēmu drošības monitorings un incidentu novēršana sadarbībā ar drošības incidentu novēršanas institūciju un amatpersonām arī ārpus darba laika;

3) publiskajā sektorā strādājošiem ir papildu stress attiecībā uz darba kvalitatīvu izpildi, jo tas būtiski var ietekmēt ikviena iedzīvotāja ikdienas dzīvi (automatizēti datu apstrādes risinājumi valsts informācijas sistēmās palīdz automatizētu lēmumu pieņemšanā, kas liedz gan izceļot vai ieceļot valstī, gan saņemt atļaujas vai piedalīties ceļu satiksmē, gan ierobežo strādāt profesijās, u.tml.), bet kvalitatīvi izpildīts darbs neietekmē mēnešalgas apmēru atšķirībā no privātā sektora, tomēr tas ietekmē atlīdzības mainīgo daļu, ja iestādei ir pieejami tam nepieciešamie finanšu resursi (novērtējuma prēmija, naudas balva, piemaksa par personisko darba ieguldījumu un darba kvalitāti, atvaļinājuma pabalsts, papildatvaļinājuma ilgums).

4) publiskā sektora vidē speciālisti pilnveido savas profesionālās zināšanas, jo tas ir nosacījums, lai strādātu IKT nozarē un sadarbotos ar privātajā sektorā IKT strādājošajiem, kuriem tiek nodrošinātas vispusīgākas un daudz dārgākas apmācības iespējas.

Tomēr atsevišķos gadījumos IeM IC ilggadējiem darbiniekiem kvalifikācija neatpaliek no speciālistu zināšanām un prasmēm IKT jomā privātajā sektorā. Tas izskaidrojams ar valsts iestāžu darbības specifiku – pārsvarā nepieciešams fokusēties uz vairāku iestāžu sadarbības jautājumu specifiku, tādējādi speciālistiem ir plašāks IKT jautājumu redzējums, tai skaitā izpratne par tehnoloģisko jauninājumu ieviešanas iespējām. Tāpēc būtiski ir šos speciālistus noturēt arī turpmāk, lai nevienlīdzīgā attieksme atalgojuma ziņā nebūtu izšķirošais faktors lēmumam par pāriešanu darbā privātajā sektorā.

[3] IeM Informācijas centra salīdzinošie novērojumi publisko darba sludinājumu portālos, publicējot savus darba sludinājumus.

Privātais sektors ir spējīgs ieguldīt ievērojamus līdzekļus jauno IKT speciālistu apmācībā, lai panāktu vēlamo kvalifikācijas nosacījumu izpildi un lai tālākais IKT projektu un procesu realizācijas process uzņēmumam būtu "veiksmes stāsts", kas, savukārt, nav iespējams valsts iestādē – speciālists ar analoģiski augstu kvalifikāciju nepieciešams uzreiz. Bieži jaunie speciālisti, kas piekrīt strādāt par pieejamo atalgojumu, nepārzina IKT izstrādes un ieviešanas metodes, kuras nepieciešamas ikdienas darba izpildē, piemēram, drošības incidentu operatīvai novēršanai. Arī izpratne par to, ka valsts informācijas sistēmu un IKT infrastruktūras veiktspēja ir tieši atkarīga no IKT speciālista, viņa zināšanu un prasmju kvalitātes, ir nepietiekama.

Ievērojot, ka jau šobrīd ir ierobežota IKT speciālistu pieejamība, kas ietekmē gan valsts, gan privāto sektoru, nepieciešams sākt tuvināt atalgojuma līmeni privātajā sektorā strādājošajiem IKT speciālistiem.

2016.gadā valstī bija vairāk kā 6180 IKT uzņēmumu privātajā sektorā, kuri 29,8 tūkst. IKT jomas speciālistu uzturēšanai izlietoja 542,2 milj. EUR (Centrālā statistikas pārvalde, 2017[4]; LIKTA, 2016 [5]). Taču 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[6]) un tas nozīmē, ka cilvēkkapitāls ar vajadzīgajām 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 apgrozījumam ir sīvi jākonkurē ar privāto sektoru (Latvijas Banka, 2016[7]).

Līdz ar to ir nekavējoties jāveic pasākumi, kas sekmētu pieredzējušu IKT nozares speciālistu noturēšanu un arī jauno nozares speciālistu piesaisti, lai nākotnē vismaz daļēji nodrošinātu arvien pieaugošo pieprasījumu pēc tiem un funkcionālo gatavību pret ārējiem apstākļiem attiecībā uz IKT infrastruktūru un valsts iedzīvotāju datiem.

Otrs svarīgākais faktors ir nākotnes IKT attīstības perspektīvu lomas pieaugums, jo tikai tā var attīstīt modernu un inovatīvu valsts pārvaldi. Taču, lai iestāde spētu īstenot IT projektu realizāciju, svarīgi ir ne tikai tos sākt savlaicīgi, bet arī pārliecināties, ka iestādes rīcībā ir atbilstošas kvalifikācijas IKT speciālisti. Būtiska virzība digitālo pakalpojumu un IKT infrastruktūras attīstības jomā ir vērojama ES 2014.– 2020.gada plānošanas periodā – IeM IC

---

[4] Centrālās statistikas pārvaldes dati par 2016.gadu "Darba spēka izmaksas". http://www.csb.gov.lv/sites/default/files/nr_18_darbaspeka_izmaksas_2016_17_00_lv.pdf.

[5] Latvijas Informācijas un komunikācijas tehnoloģiju asociācija. 2016. LIKTA 18.gadskārtējā konference "Sabiedrības izaicinājumi digitālajā laikmetā". https://www.likta.lv/LV/Documents/Signe%20Balina%20LIKTA%20konference%202016_final.pdf.

[6] Certus pētījums .2017. "Latvijas konkurētspējas ziņojums. Informācijas un komunikācijas tehnoloģijas nozare Latvijā". http://certusdomnica.lv/wp-content/uploads/2017/03/Certus_InformacijasUnKomunikacijasTehnologijas_2016.pdf.

[7] Latvijas Bankas pētījums. 2016. "Latvijas pakalpojumu eksportētāju ekonomiskais raksturojums". https://www.bank.lv/images/stories/pielikumi/publikacijas/petijumi/p_6_2015_lv.pdf.

plāno piedalīties ES IKT projektos, kuru izmaksas ir 13,2 milj. EUR. Tāpēc vēl svarīgāk ir nodrošināt kvalificētu IKT speciālistu palikšanu iestādē, nodrošinot konkurētspējīgu atalgojumu.

Iepriekšējos gados IeM IC kopējā personāla mainība ik gadu nav pārsniegusi 6 – 7%, bet 2016.gadā tā ir sasniegusi augstāko līmeni – 13%, un ir dubultojusies attiecībā pret iepriekšējo kalendāro gadu (2015.gadā darbinieku mainība bija 7%) (IeM IC, 2017[8]). Līdz 2016.gadam augstākā personāla mainība ir bijusi ekonomiskās lejupslīdes periodā (2011.gadā – 11%), bet pēc tam bijusi praktiski nemainīga līdz 2016.gadam. IeM IC aptaujātie faktiskie iemesli nodarbināto aiziešanai ir salīdzinoši zemā mēnešalga.

Kopējais atalgojuma palielinājuma mērķis ir veicināt atalgojuma konkurētspēju un paaugstināt iespēju noturēt iestādē nodarbinātos IKT profesionāļus ar kvalifikāciju, prasmēm un pieredzi, kā arī veicināt jauno IKT speciālistu piesaisti, sekmējot tehnoloģisko inovāciju ieviešanu un produktivitātes paaugstināšanu iekšlietu nozarē. Tādējādi tiks veicināta arī kopējo inovatīvo IKT risinājumu skaita palielināšanās, IKT infrastruktūras drošības īpatsvara pieaugums un IKT nozares izaugsme valsts sektorā.

1.4. IeM IKT infrastruktūras aizsardzība

IeM iekšējais datu pārraides tīkls 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, tiek izmantota virkne ar moderniem šobrīd pasaulē atzītiem un efektīviem drošības risinājumiem:

1. Ielaušanās noteikšanas un novēršanas sistēmas (IDS un IPS) Cisco Sourcefire, kas nodrošina gan no ārpuses veikto uzbrukumu mēģinājumu (incidentu) atklāšanu un bloķēšanu, gan arī no IeM datortīkla iekšpuses ierosinātos incidentus (pārsvarā IeM datortīkla iekšienē incidentus izraisa inficēti datori).
2. Ugunsmūru un virtuālā privātā tīkla risinājumi (Firewalls, VPNs) - starpsavienojumu izveidei un aizsardzībai tiek izmantots VPN risinājums un ugunsmūris Checkpoint.
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 aizdomīgu datu apmaiņu (saturu vai savienojuma mērķi). Salīdzinājumā ar citiem IeM IC izmantotajiem drošības rīkiem, šī rīka priekšrocība ir iespēja izmantot komerciāli nepieejamus informācijas avotus par ļaunatūru pazīmēm.

[8] IeM IC gada publiskais pārskats par 2016.gadu.
http://www.ic.iem.gov.lv/sites/default/files/IeMIC_Gada_publiskais_parskats_2016.pdf.

4. IeM iekšējā tīkla plūsmu anomāliju analīzes rīks Lancope StealthWatch, 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. Ārējā tīklā pieejamo IKT resursu papildus aizsardzībai pakāpeniski tiek uzsākta QualysGuard Vulnerbility management rīka izmantošana.
7. IeM iekšējam datu pārraides tīklam pieslēgto darba staciju aizsardzībai pret nevēlamu programmu (ļaunatūru) nonākšanai IeM datortīklā tiek izmantota antivīrusa programmatūru Kaspersky Endpoint Security.
8. 2016.gadā ir iegādāts un šogad ekspluatācijā tiks nodots mobilo iekārtu (viedtālruņu un planšetdatoru) drošības risinājums (MDM).
9. 2016.gadā ir iegādāts un šogad ekspluatācijā tiks nodots žurnālfailu automatizētas analīzes un kontroles rīks (SIEM).
10. Fizisko tīkla pieslēgumu aizsardzībai (802.1x on switch port security) uzsākta Cisco ISE rīka ieviešana.

Šeit minēto drošības rīku uzraudzību un reakciju uz trauksmes paziņojumiem nodrošina IeM IC personāls paralēli citiem pienākumiem IKT infrastruktūras uzturēšanas jomā. No drošības rīkiem saņemtās trauksmes un atskaites tiek analizētas izlases kārtībā.

Piekļuve pie atsevišķiem šeit minētajiem drošības rīkiem IeM un padotības 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.

1.5. Priekšlikumi situācijas uzlabošanai

Lai mainītu iepriekš raksturoto situāciju, IeM IC sagatavojis attiecīgo jauno politikas iniciatīvu (JPI) un prioritāro pasākumu pieteikumus, kas tika iekļauti IEM pieteikumu sarakstā, piemēram:

- IT personāla atlīdzības paaugstināšana – attiecīgs minimāli nepieciešamā papildu finansējuma pieprasījums (ziņojuma 1.pielikuma 2.pasākums);
- Vienotas informācijas aizsardzības pārvaldības sistēmas izveidošana IeM un tās padotības iestādēs (DLP) – finansējums tika prasīts jau kopš 2010.gada (kā jaunās politikas iniciatīva – kopš 2013.gada) (ziņojuma 1.pielikuma 7.pasākums);
- IeM padotības iestāžu rīcībā esošās datortehnikas plānveida nomaiņa (atjaunošana) – finansējums tika prasīts, sagatavojot un iesniedzot attiecīgu

jaunās politikas iniciatīvu – kopš 2013.gada (ziņojuma 1.pielikuma 1A.pasākums);

- Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana – finansējums tika prasīts, sagatavojot un iesniedzot attiecīgu jaunās politikas iniciatīvu – kopš 2013.gada (ziņojuma 1.pielikuma 1B.pasākums).

2. DROŠĪBAS INCIDENTS

2.1. Priekšvēsture

2014.gada martā, pateicoties Cert.lv sensora ziņojumam, tika konstatēta aizdomīga komunikācija no IeM IKT infrastruktūras ar publisko tīklu (internetu). Komunikācija notika no gandrīz 50 datoriem, no kuriem 1 bija VRS Ludzas pārvaldē, bet pārējie – dažādās VP struktūrvienībās – gan VP datoros Rīgā, Čiekurkalna 1.līnijā 1, k- 4, gan VP Rīgas reģiona pārvaldes iecirkņos, gan VP Latgales reģiona pārvaldē. Visi datori tika atslēgti no datortīkla un pārinstalēti, 2 no tiem noteiktu laiku tika saglabāti, lai Cert.lv speciālisti varētu tos padziļināti pārbaudīt. Arī 2015.gadā tika atklāta aizdomīga aktivitāte vēl 16 VP Latgales reģiona datoros un 3 VRS datoros (VRS Galvenā pārvalde, VRS Ludzas pārvalde).

Vairākos gadījumos tika konstatēts, ka attiecīgajos datoros nestrādāja antivīruss, t.sk., sakarā ar datora jaudas nepietiekamību un nepilnībām to pārvaldībā (konfigurācijas iestatījumos). Arī 2016.gadā tika konstatēta vairāku datoru "aizdomīga komunikācija" ar publisko tīklu (internetu). Sadarbībā ar Cert.lv tika uzsākta attālināta visu IeM un padotības iestāžu datoru padziļināta pārbaude, lai noskaidrotu iespējamās ļaunatūras klātbūtnes pazīmes. Tika pārbaudīti aptuveni 70% IeM datortīklam pieslēgtu datoru, no kuriem kā inficētus ar ļaunatūru Cert.lv speciālisti atzina 24 datorus.

2.2. Cert.lv atklājumi

Cert.lv speciālisti ir atklājuši, ka ļaunatūra IeM datortīklam pieslēgtajos datoros darbojas vismaz kopš 2008.gada. Ļaunatūra ir izplatījusies gan ar datortīkla (interneta) starpniecību, gan, izmantojot pārnēsājamos datu nesējus. Atsevišķos gadījumos ir konstatēts, ka IeM izmantotā antivīrusu programmatūra nav konstatējusi ļaunatūru, kas var liecināt par antivīrusu programmatūras neuzticamību. Pastāv aizdomas, ka ļaunatūra būtu varējusi iegūt IeM datortīkla priviliģētā konta (administratora) tiesības, kā arī, iespējams, ir nosūtījusi uz ļaunatūras vadības centru IeM datortīklā apstrādājamo informāciju (ir identificēti auditācijas pieraksti par šifrētas informācijas izsūtīšanu, bet nav identificēts konkrēts informācijas apjoms). Cert.lv uzskata, ka IeM datortīkla infrastruktūra ir pilnībā kompromitēta.

2.3. Neatliekami veicamie pasākumi

Lai risinātu radušos situāciju, Cert.lv speciālisti iesaka efektīvāk pārvaldīt esošos drošības rīkus, piesaistot šim mērķim papildu cilvēkresursus un pilnā apjomā pārbūvējot visu IeM IKT lietotāju darba vides pārvaldības infrastruktūru. Tomēr IeM IC skatījumā IKT infrastruktūras pilnīga pārbūve nebūs efektīvs risinājums, jo prasīs neadekvāti liela apjoma investīcijas (B.variants), turklāt negarantējot ļaunatūras iznīcināšanu IeM datortīklā. Papildus cert.lv atbalsta arī citu risinājumu ieviešanu drošības incidentu izmeklēšanai (A.variants).

IeM IC rīcībā jau ir vairāki moderni šobrīd pasaulē atzīti un efektīvi drošības risinājumi, taču galvenokārt tiek izmantota tikai šo rīku automātiskās darbības iespēja, administratoram, reaģējot uz trauksmes paziņojumiem tikai izlases kārtībā. Rīku pilnvērtīgai izmantošanai būtu nepieciešama drošības administratoru veikta uzraudzība. Papildus iepriekš minētajam IeM IC pēc IeM IKT resursu centralizācijas jau ir identificējis vairākus trūkumus IeM IKT resursu pārvaldībā un drošības nodrošināšanā, tāpēc tiek plānots veikt pasākumus šādās jomās (1. tabulā):

1. Drošas lietotāju darba vides nodrošināšana.
2. Cilvēkresursu kapacitātes un kvalitātes paaugstināšana.
3. Centrālās infrastruktūras aizsardzība.
4. Datu pārraides infrastruktūras aizsardzība.

Ņemot vērā saņemto informāciju par atklāto ļaunatūru, tās uzbrukuma vektoru un izplatīšanās metodēm, īpaša uzmanība pievēršama drošas lietotāju darba vides nodrošināšanai, tāpēc IeM IC ieskatā, lai novērstu radušos situāciju, jāpanāk, lai tiktu izveidota homogēna (minimizēts izmantojamo datoru operētājsistēmu versiju skaits) lietotāju darba vide, tiktu nodrošināta efektīva tās pārvaldība, nepārtraukta drošības uzraudzība un incidentu novēršana, galvenokārt piesaistot tam atbilstošus cilvēkresursus.

Drošas lietotāju darba vides izveidei tiek piedāvāti 2 risinājuma varianti:

A- infrastruktūras sakārtošana un drošības uzlabošana – datortehnikas plānveida nomaiņa, ietverot daļēju virtualizētu darba vietu ieviešanu.

B- jaunas izolētas infrastruktūras ieviešana, aizstājot esošo – masveida centralizēti pārvaldītu virtualizētu darba vietu risinājumu ieviešana.

Minēto pasākumu nepieciešamība ir apspriesta un kopumā sakrīt ar Cert.lv redzējumu IeM IKT infrastruktūras drošības uzlabošanai.

1.tabula

Veicamie pasākumi atbilstoši A un B risinājuma variantiem

Pasākums/apakšpasākums	Varianti	
	A	B
1. Drošas lietotāju darba vides nodrošināšana		
Datortehnikas plānveida nomaiņa, ietverot daļēju virtuālu darba vietu ieviešanu (katru gadu nomainot 20% datortehnikas), tādejādi	+	

nodrošinot, ka tiek nomainīta jau nolietotā datortehnika, datoros tiek izmantota tikai viena - jaunākā operētājsistēma		
Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana (*ieviešana 5 gadu laikā) – jaunu datoru vietā tiek palielinātas datu centru jaudas, visas datoru operētājsistēmas tiek darbinātas datu centrā		+
Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana, kas ļautu efektīvāk pārvaldīt (noteikt, instalēt) ne tikai operētājsistēmu, bet arī citas lietotāju programmatūras drošības ielāpus	+	+
Vienotas informācijas aizsardzības pārvaldības sistēmas izveidošana IeM un tās padotības iestādēs (DLP) (*ieviešana 3 gadu laikā), ar kuras palīdzību varētu kompleksi monitorēt jebkādus informācijas noplūdes ceļus un veidus visā IeM IKT infrastruktūrā	+	+
2. Cilvēkresursu kapacitātes un kvalitātes paaugstināšana		
Datordrošības struktūrvienības izveide	+	+
IKT personāla atlīdzības konkurētspējas uzlabošana, novēršot personāla mainību un pieredzējušu IT ekspertu aizplūšanu uz privāto sektoru	+	+
Personāla apmācība (gan drošības, gan infrastruktūras drošas un efektīvas pārvaldības jomā)	+	+
3. Centrālās infrastruktūras aizsardzība		
Priviliģēto kontu pārvaldības risinājums – efektīvākai IT administratoru, kam ir augstas privilēģijas darbā ar sistēmām, darba vides aizsardzībai, minimizējot administratoru kontu uzlaušanas iespējas	+	+
Sistemātisku drošības testu veikšana	+	+
4. Datu pārraides infrastruktūras aizsardzība		
Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve (*ieviešana 5 gadu laikā) nodrošinot autentifikāciju ne tikai datorā, bet arī tīkla līmenī liedzot jebkādas iespējas pieslēgt tīklam neidentificēta iekārtas	+	+
Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (*ieviešana 3 gadu laikā), kas garantētu datu plūsmas kontroli un tīkla līmeņa datu plūsmas šifrēšanu starp IeM un padotības iestādēm (t.sk.atsevišķām struktūrvienībām), kas savienotas ar publisko datu pārraides tīklu starpniecību.	+	+

2.tabula

A un B risinājuma variantu salīdzinājums

	A variants – infrastruktūras sakārtošana un drošības uzlabošana	**B variants –** jaunas izolētas infrastruktūras ieviešana, aizstājot esošo
IEGUVUMI	1. Neprasa lielus cilvēkresursu ieguldījumus ieviešanai, bet pakāpeniski ierastajā kārtībā tiek paaugstināts drošības līmenis un informācijas aizsardzības pakāpe esošajai infrastruktūrai. 2. Ilgtermiņā pastāv iespēja datortehnikas iegādei paredzētā finansējuma ietvaros veikt virtualizētas infrastruktūras izbūvi nevis masveidā, bet to plānojot un izmantojot tikai atsevišķās IeM padotības iestāžu struktūrvienībās, kur tai būtu visaugstākā pievienotā vērtība. 3. Ievērojami mazāki izdevumi darbstaciju licencēšanā, jāiegādājas tikai Windows OEM licences	1. Izveidota izolēta vide ar augstu informācijas aizsardzības pakāpi. 2. Daudz vieglāka darba staciju pārvaldība – visas operācijas veicamas datu centrā ar automatizētiem rīkiem.

TRŪKUMI	1. Salīdzinoši augstāks risks (pretstatā B variantam), ka ļaunatūra tiek pilnībā likvidēta, jo infrastruktūra netiek būvēta no jauna pilnībā izolētā vidē. 2. Sarežģītāka darbstaciju pārvaldība, ilgāks operāciju (programmatūras instalēšana, atkļūdošana, u.t.l.) izpildes laiks. 3. Informācijas apstrāde notiek datoros, nevis centralizēti datu centra ietvaros, līdz ar to palielinās informācijas noplūdes riski.	1. Augstākas ieviešanas izmaksas (datu centru infrastruktūras iegādei). 2. Ļoti sarežģīta ieviešana, kas šobrīd nav detalizēti izpētīta, kā arī nav apzināts, vai visi iestāžu darba procesi būs veicami virtualizētās darba stacijās. 3. Iespējams, ne visos IeM objektos būs iespējams izmantot virtuālās darba stacijas tīkla caurlaides nepietiekamības dēļ un būs nepieciešamas papildu investīcijas tās uzlabošanā. 4. Neskatoties uz plašākām infrastruktūras izolācijas iespējām, joprojām pastāv augsts risks, ka infrastruktūra var tikt inficēta, jo dati no "vecās infrastruktūras" būs jāpārnes. 5. Salīdzinot ar Windows OEM licencēšanas modeli, dārgākas operētājsistēmu licences, kuras nav nopērkamas, bet ir pieejamas tikai nomā. Jāuzņemas ilgtermiņa finanšu saistības. Pārtraucot licenču nomu, zūd tiesības izmantot virtualizēto darba vidi visiem lietotājiem. Infrastruktūras pārvaldībai nepieciešama darbinieku apmācība specifisku virtualizācijas produktu pielietošanā, taču esošais atalgojums neļauj apmācītus pieredzējušus speciālistus ilgstoši noturēt darbā valsts iestādē.
IZMAKSAS	Ieviešanas izmaksas - 16 877 890 *euro*	Ieviešanas izmaksas - 22 675 090 *euro*

Plānoto pasākumu saraksts prioritārā secībā un izmaksu kopsavilkums – ziņojuma 1.pielikumā. Plānoto pasākumu detalizēts prognozēto izmaksu aprēķins un apraksts – ziņojuma 2.pielikumā. Pasākumu plānoto izdevumu tāmes kopsavilkums sadalījumā pa izdevumu kodiem atbilstoši ekonomiskajām kategorijām (EKK) – ziņojuma 3.pielikumā.

Ņemot vērā pasākumu īstenošanai nepieciešamos cilvēkresursus un izmaksas, **Iekšlietu ministrija ierosina īstenot A risinājuma variantu**.

3. SECINĀJUMI

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

IeM IKT infrastruktūrā turpinās novecojušas datortehnikas izmantošana, kā arī ražotāja neatbalstītas programmatūras izmantošana (piemēram, Windows XP operētājsistēmas).

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

Ir apstiprināta ļaunatūras klātbūtne atsevišķās IeM IKT infrastruktūrā ietilpstošās darbstacijās. Nav pārliecinoša apstiprinājuma par ļaunatūras izplatīšanās mērogu, taču kiberdrošības jomā tādu apstiprinājumu ne vienmēr ir iespējams iegūt.

Ņemot vērā iepriekš minēto, pēc iespējas ātrāk jāuzsāk IeM IKT infrastruktūras drošības plānveida, mērķtiecīga uzlabošana un konstatēto trūkumu novēršana atbilstoši A. variantam.

Neveicot šajā informatīvajā ziņojumā minētos pasākumus, ļaunatūras izplatība ar lielu varbūtību turpināsies un IeM datortīkls arī turpmāk būtu jāuzskata par kompromitētu.

Iekšlietu ministrs Rihards Kozlovskis

Vīza: Valsts sekretārs Dimitrijs Trofimovs

23.08.2017. 14:22
89453
S.Kanteruks, 67208634
sergejs.kanteruks@ic.iem.gov.lv
A.Kronberga, 67208712
arta.kronberga@ic.iem.gov.lv
20.07.2017 16:00

1.pielikums

Plānoto pasākumu saraksts prioritārā secībā un izmaksu kopsavilkums

	Pasākums	Ieviešanas ilgums, gadi	Kopējās ieviešanas izmaksas 2017-2022[9]	2017	2018	2019	2020	2021	2022 un turpmāk katru gadu [10]
1A	Datortehnikas plānveida nomaiņa	5	8 505 000	2 025 000	1 620 000	1 620 000	1 620 000	1 620 000	(1 620 000)
1B	Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana	3	14 302 200	-	-	-	4 767 400	4 767 400	4 767 400
2.1	Datordrošības struktūrvienības izveide	1	183 198	-	183 198	(183 198)	(183 198)	(183 198)	(183 198)
2.2	IT personāla atlīdzības konkurētspējas uzlabošana	1	610 346	(146 483)	610 346	(610 346)	(610 346)	(610 346)	(610 346)
2.3	Apmācības	1	19 929	(6 075)	19 929	(19 929)	(19 929)	(19 929)	(19 929)
3	Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana	1	139 200	-	139 200	(139 200)	(139 200)	(139 200)	(139 200)
4	Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve	4	3 449 250	756 000	897 750	897 750	897 750+ (75 600)= 973 350	(128 400)	(181 200)
5	Priviliģēto kontu pārvaldības risinājums	1	101 156	-	101 156	(18 174)	(18 174)	(18 174)	(18 174)
6	Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai	3	969 811	-	434 342	116 934+ (122 646)= 239 580	418 535+ (156 018)= 574 553	(156 018)	(156 018)
7	Vienotas informācijas aizsardzības pārvaldības sistēmas izveidošana IeM un tās padotības iestādēs (DLP)	3	2 880 000	-	-	960 000	960 000+ (144 000)= 1 104 000	960 000+ (288 000)= 1 248 000	(432 000)
8	Drošības testu veikšana	1	20 000	-	20 000	(20 000)	(20 000)	(20 000)	(20 000)
	KOPĀ A variants		16 877 890	2 933 558	4 025 921	4 708 177	5 262 750	4 143 265	3 380 065
	KOPĀ B variants	-	31 180 090	x	x	x	x	x	x

[9] Norādīti tikai ieviešanas izdevumi, neiekļaujot nepieciešamos bāzes izdevumus, t.sk.uzturēšanai, nākamajiem gadiem un par 2017.gadu - 2.2. un 2.3.pasākumam (nepilns gads) (iekavās); izmaksām ir informatīvs raksturs, lai salīdzinātu A un B varianta izmaksas

[10] Turpmāk katru gadu-iekavās norādītie izdevumi

2.pielikums

Plānoto pasākumu detalizēts izmaksu aprēķins apraksts

Nr.	Pasākums	Apraksts	Ieviešanas izmaksas	Uzturēšanas izmaksas
1A	Datortehnikas plānveida nomaiņa	Lai nodrošinātu adekvātu informācijas aizsardzību, lietotāju darbstacijām jābūt nodrošinātām ar izmantotās programmatūras aktuālajiem drošības jauninājumiem. Ievērojot, ka IeM programmatūra (Windows) netiek nomāta, bet izmantotas lētākas OEM licences, kas tiek iepirktas kopā ar datoru, to ir iespējams panākt, nepieļaujot novecojušas datortehnikas izmantošanu. Optimālais datortehnikas dzīves cikls ir 3-5 gadi. Tāpēc katru gadu jāparedz vismaz 20% datortehnikas nomaiņa. Pirmajā pārskata gadā jānomaina visa uz šo brīdi drošības prasībām neatbilstošā datortehnika un programmatūra. **Nepieciešamais finansējuma apjoms iekļauts IeM IC 2018. gada prioritāro pasākumu saraksta 2. pasākumā.**	**2017.gadā:** -1620 gab. datori x 820 EUR = 1 328 400 (EKK 5238); -300 gab portatīvie datori x 1350 EUR=405 000 (EKK 5238) -1620 gab monitori x180 EUR=291 600 (EKK2312) KOPĀ: **2 025 000 EUR** **2018.gadā un turpmāk katru gadu:** -1620 gab. datori x 820 EUR = 1 328 400 (EKK 5238); -1620 gab monitori x180 EUR=291 600 (EKK 2312) KOPĀ: 1 620 000 EUR	Ieviešana plānota tā, ka katru gadu tiek nomainīti 20% no visas datortehnikas, tādejādi nepieļaujot par 5 gadiem vecāku datoru ekspluatāciju
1B	Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana	Izolēts tīkls ar virtualizētu darbstaciju infrastruktūru (VDI), kur visa lietotāju informācija tiek glabāta centralizēti, tadejādi nodrošinot tās efektīvāku pārvaldību un aizsardzību. Risinājums nav ieviešams 100 % visām darba vietām, jo noteikti būs darba procesi iestādēs, kas nav veicami ar virtualizētas darbstacijas palīdzību (aprēķini veikti 7500 darba vietām). Risinājuma sarežģītības dēļ un pieejamo cilvēkresursu ietvaros **ieviešana var tikt uzsākta tikai no 2020. gada, realizējot to 3 gados.**	**2020 gadā**: -servertehnika 25 gab. x 22 000 EUR = 550 000 EUR (EKK 5238); -VDI virtualizācijas licences komplekts 250 gab. x 6 100 EUR = 1 525 000 EUR (EKK 5238); -Datu glabātuves (SSD disku apakšsistēma) 2 gab x 67 000 EUR = 134 000 EUR (EKK 5238); -Plānie klienti 2500 gab. x 490 EUR = 1 225 000 EUR (EKK 5238); -VDA (Virtual desktop access) Windows licenču noma 2500 gab. x 360 EUR = 900 000 EUR (EKK 2252) - VDI infrastruktūras ieviešanas (t.sk.	Virtualizētu darbstaciju infrastruktūras dzīves optimālais cikls ir 6 līdz 7 gadi, pēc kā jāparedz serveru infrastruktūras, datu krātuvju un plāno klientu nomaiņa. Ieviešanas izmaksas aprēķinātas ar iekļautu 3 gadu atbalstu. Ikgadējie uzturēšanas izdevumi pēc visas infrastruktūras pilnīgas ieviešanas: Servertehnikai un datu glabātuvēm - 10% apmērā no iegādes izmaksām jeb 205 200 EUR/gadā (EKK2243), VDA Windows licenču nomas izmaksas sastāda 7500 gab. x 120 EUR = 900 000 EUR/gadā (EKK2252), VDI virtualizācijas licenču atbalsts - 20 % no licenču iegādes izmaksām jeb 915 000 EUR/gadā (EKK2252). **Kopā: 2 020 200 EUR/gadā**

			loģistikas) un apmācības pakalpojumi 10 % no infrastruktūras izmaksām = 433 400 EUR (EKK 2259) Kopā: 4 767 400 EUR **2021. gadā:** 4 767 400 EUR **2022. gadā:** 4 767 400 EUR **Kopā: 14 302 200 EUR**	
2.1	Datordrošības struktūrvienības izveide	Izveidot struktūrvienību, kas koordinētu un nepastarpināti nodrošinātu informācijas un IKT resursu aizsardzību. Galvenās funkcijas: 1. Nepastarpināti veikt IeM IC rīcībā jau esošo drošības risinājumu (Firewall, IDS, IPS, SIEM, MDM, Lancope, u.c.) darbības kontroli un drošības paziņojumu apstrādi. 2. Nepastarpināti nodrošināt drošības incidentu reģistrēšanu, izmeklēšanu un analīzi. 3. Nepastarpināti kontrolēt piekļuvi IeM IKT infrastruktūrai un informācijai (MDM, Checkpoint, Paroļu reģistrs, MS Active directory, u.c.). 4. Organizēt Informācijas centra informācijas un tehnisko resursu fiziskās un loģiskās aizsardzības pārvaldību – normatīvā regulējuma izstrāde, izpildes kontrole. 5. Proaktīvi vērtēt plānojamās informācijas sistēmu izmaiņas un to ietekmi uz informācijas drošību (risku analīze); **Iespējams, sākot ar 2018. gadu, pietiekoša finansējuma ietvaros.**	-	19.5, IV 12.mēnešalgu grupa mēnešalga 1 647 x 12 mēn. = 19 764 EUR x 6 darbinieki = 118 584 EUR (EKK 1119) Piemaksa par papildu darbu 118 548 EUR x 10% =11 858 EUR (EKK 1146) Prēmijas, naudas balvas un materiālā stimulēšana 118 548 EUR x 10% =11 855 976,40 EUR x 6 darbinieki = 11 859 EUR (EKK 1148) Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas 24 705 EUR x 23.59%= 5 827,91 EUR x 6 darbinieki = 34 968 EUR (EKK 1210) Darba devēja pabalsti un kompensācijas, no kuriem aprēķina ienākuma nodokli, valsts sociālās apdrošināšanas obligātās iemaksas 118 584 EUR x 5%= 5 929EUR (EKK 1221) **Kopā atlīdzība 6 darbiniekiem: 183 198 EUR/gadā** **Cilvēku skaits aprēķināts ņemot vērā, ka tiek ieviesti 3. – 5. punktā minētie papildu drošības risinājumi.**
2.2	IKT personāla atlīdzības konkurētspējas uzlabošana	IKT infrastruktūru uzturošā personāla atalgojuma konkurētspējas uzlabošana, lai samazinātu kvalificēta personāla aizplūšanu un saglabātu iestādē uzkrāto zināšanu bāzi. Tādējādi tiks nodrošināts pilna IKT mijiedarbības komponentu (informācija ⇔ cilvēks) modeļa īstenošana IKT		Darbinieki ar sekojošām amatu saimēm, līmeņiem un mēnešalgu grupām: 1. 18.6 IA 5.mēnešalgu grupa mēnešalga 3 kategorija 802 EUR x 0,8 x 5 amata vietas x 12 mēneši = 38 496 EUR - 37 200 EUR (budžets 2017.gadā) = 1 296 EUR

		infrastruktūras drošā pārvaldībā. Modelis paredz nodrošināt IKT infrastruktūras veiktspējas (informācijas sistēmas un saturs) un lietotāju (lietojamība un inženiertehnoloģisko risinājumu derīgums) pārvaldību. IKT personāls realizē IKT infrastruktūrā risinājumus, lai realizētu daudzpakāpju pieeju: - lietotājorientēto pieeju, - informācijas tehnoloģijas (datorzinātnes), - fizisko pieeju (t.sk., tehnisko sistēmpieeju un inženiertehniskos risinājumus), lai nodrošinātu visu komponenšu savstarpējo sadarbību IKT infrastruktūras drošības veicināšanā. Darbinieki ar 18.saimi (**informācijas apkopošana un analīze**) nodrošina: - informācijas lietošanas uzvedības apkopošanu; - informācijdarbības izpēti (informācijas meklēšanas ilgums un metodes; nozīme, kāda tiek piešķirta izmantojamajām datu kategorijām; lietotāju informacionālā uzvedība; informācijas sistēmu vienlaicīgas lietošanas modeļu identificēšana); - informacionālās uzvedības analīzi (ātrākie, plašākie, dziļākie informācijas saņēmēji un izplatītāji no informācijas sistēmās visā IT infrastruktūrā kopā ar raksturīgu un neraksturīgu darbību izpēti); - infometrijas uzdevumu izpildi (informācijas kvantitatīvu izpēti) – cik daudz, kurš ir produktīvāks (aktīvāks) informācijas izplatītājs un kā attīstījusies informācijas kustība starp iestādēm un		2. 18.6 IB un 19.6 I 6.mēnešalgu grupa mēnešalga 3 kategorija 899 EUR x 0,8 x 6 amata vietas x 12 mēneši = 51 783 EUR - 45 360 EUR (budžets 2017.gadā) = 6 422 EUR 3. 18.1 I ; 18.6 II un 19.4 I 7.mēnešalgu grupa mēnešalga 3 kategorija 996 EUR x 0,8 x 31 amata vietas x 12 mēneši = 296 410 EUR - 265 320 EUR (budžets 2017.gadā) = 31 090 EUR 4. 19.2 I; 19.5 IIA 8.mēnešalgu grupa mēnešalga 3 kategorija 1093 EUR x 0,8 x 15 amata vietas x 12 mēneši = 157 392 EUR - 141 300 EUR (budžets 2017.gadā) = 16 092 EUR 5. 18.6 II; 19.5 IIB, 20 II 9.mēnešalgu grupa mēnešalga 3 kategorija 1190 EUR x 0,8 x 71 amata vietas x 12 mēneši = 811 104 EUR - 649 080 EUR (budžets 2017.gadā) = 162 024 EUR 6. 19.2 II; 19.4 III; 19.5 IIIA; 20 III; 52 II 10.mēnešalgu grupa mēnešalga 3 kategorija 1287 EUR x 0,8 x 83 amata vietas x 12 mēneši = 1 025 482 EUR - 918 288 EUR (budžets 2017.gadā) = 107 194 EUR 7. 19.4 IV; 19.5 IVA; 20 IV 12.mēnešalgu grupa mēnešalga 3 kategorija 1647 EUR x 0,8 x 39 amata vietas x 12 mēneši = 616 637 EUR - 554 088 EUR (budžets 2017.gadā) = 62 549 EUR 8. 19.3 IIIB; 20 V; 36 IV 13.mēnešalgu grupa mēnešalga 3 kategorija 1917 EUR 0,8 x 3 amata vietas x 12 mēneši = 55 210 EUR - 46 800 EUR (budžets 2017.gadā) = 8 410 EUR Kopā pārējo darbinieku mēnešalga (darba alga)

		struktūrvienībām, ietekmējot IT infrastruktūras darbību. Darbinieki ar 19.saimi (**informācijas tehnoloģijas**) veic apkopotās un izanalizētās informācijas apstrādi, lai nodrošinātu: - koplietošanas modeļu izstrādi IT jomā; - IKT mērķarhitektūrā iekļauto projektu procesu uzraudzību un īstenošanu; - programmnodrošinājumu administrēšanu; - tehnisko risinājumu un infrastruktūras stāvokļa novērtēšanu un analīzi. Darbinieki ar 20.saimi (**inženiertehniskie darbi**) nodrošina: - nestandarta inženiertehniskās problēmas risinājumus, ieviešot informācijas tehnoloģijas; - inženiertehnisko risinājumu uzturēšanu; - piemērotāko inženiertehnisko risinājumu attīstības iespēju analīzi. Darbinieki ar 36.saimi (**politikas plānošana**), izanalizējot informācijas apkopošanas un analīzes rezultātus, informācijas tehnoloģiju un inženiertehnoloģisko risinājumu attīstību attiecībā pret iestādes resursiem, nodrošina: - IT mērķarhitektūras attīstības plānošanu, veicinot nākotnes risku novēršanas rīcības plānu izstrādi un īstenošanas pārraudzību; - koplietošanas moduļu izmantojošo iestāžu īpatsvara palielināšanu; - nestandarta IT risinājumu ieviešanas plānošanu, pilnveidojot publiskās pārvaldes procesus, palielinot e-prasmes un saglabājot esošā līmenī un attīstot IT infrastruktūras drošības līmeni. Izdevumi atlīdzībai aprēķināti saskaņā ar Ministru kabineta 2009.gada 15.decembra instrukcijas Nr.19 „Tiesību akta projekta sākotnējās ietekmes izvērtēšanas kārtība”		(EKK1119) 395 077 EUR Piemaksa par papildu darbu (EKK1147) 10% no gada mēnešalgas x 395 077 EUR = 39 508 EUR Prēmijas un naudas balvas (EKK1148) 10% no gada mēnešalgas x 395 077 EUR = 39 508 EUR Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas (EKK1210) 23,59% no 493 847 EUR = 116 499 EUR Darba devēja pabalsti un kompensācijas, no kuriem aprēķina iedzīvotāju ienākuma nodokli un valsts sociālās apdrošināšanas obligātās iemaksas (EKK1221) 5% no gada mēnešalgas x 395 077 EUR = 19 754 EUR **Kopā atlīdzība 2018.gadā un turpmāk katru gadu 395 077 EUR+39 508 EUR +39 508 EUR + 116 499 EUR+19 754 EUR = 610 346 EUR** **Kopā atlīdzība 2017.gada trīs mēnešiem 146 483 EUR** Pārējo darbinieku mēnešalga (darba alga) (EKK 1119) 395 077 EUR x12 mēneši x 3 mēneši = 98 769 EUR Piemaksa par papildu darbu (EKK1147) 10% no gada mēnešalgas kopsummas x 98 769 EUR = 9 877 EUR Prēmijas un naudas balvas (EKK1148) 10% no gada mēnešalgas kopsummas x 98 769 EUR = 9 877 EUR

		prasībām 253 darbiniekiem, kuri nodarbināti informācijas un komunikācijas tehnoloģiju risinājumu un infrastruktūras uzturēšanas, pārvaldības un attīstības nodrošināšanas jomā 32 923 EUR/mēn. x 12 mēn. = 395 077 EUR (aprēķins veikts mēnešalgu grupas 3.kategorijas maksimālajai mēnešalgai piemērojot koeficientu 0,8). **Iespējams ieviest, sākot ar 2017. gada septembri.**		Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas (EKK1210) 23,59% no 118 523 EUR = 27 960 EUR
2.3	Apmācības	Personāla kvalifikācijas paaugstināšana informācijas un komunikācijas tehnoloģiju drošības jomā. Regulāras apmācības ļautu nodrošināt personāla zināšanu aktualitāti IT drošības jomā, kā arī kalpotu kā papildus motivators IKT personāla noturēšanai. Uz doto brīdi drošības jomā kvalifikācijas paaugstināšana faktiski nenotiek.		Paredzēts katru gadu 10 padziļināti kursi (izmaksas no 1500 EUR līdz 2000 EUR) informācijas sistēmu drošības jomā un 7 pamata līmeņa kursi (līdz 1000 EUR), tādejādi nodrošinot vidēji 15 darbinieku apmācību katru gadu. Ņemot vērā kursu grafiku, 2017.gadā būtu iespējams veikt daļēju apmācību (http://www.bda.lv): 2 kursi "CyberSec First Responder: Threat Detection and Response (CFR) x 1 513 EUR = 3 025 EUR 7 kursi "IT un datu drošība (IT_dd) x 436 EUR = 3 050 EUR **Kopā 2017.gadā: 6075 EUR (EKK 2235)** Aprēķina piemērs, vadoties no aktuālajiem tirgus piedāvājumiem (http://www.bda.lv): 1 kurss "Sertificēts informācijas drošības vadītājs(CISM), 40h x 1 936 EUR = 1 936 EUR 1 kurss "Sertificēts ielaušanās testēšanas Inženieris (CPTE), 40h x 1 634 EUR = 1 634 EUR 2 kursi "Sertificēta informācijas sistēmu drošības profesionāļa (CISSP) sagatavošanas kurss, 40h" x 1 815 EUR = 3 630 EUR 2 kursi "Certified Ethical Hacker v.9 (CEH), 40h" x 1 815 EUR = 3 630 EUR

				2 kursi "CompTIA® Advanced Security Practitioner (CASP)" x 1 513 EUR = 3 025 EUR 2 kursi "CyberSec First Responder: Threat Detection and Response (CFR) x 1 513 EUR = 3 025 EUR 7 kursi "IT un datu drošība (IT_dd) x 436 EUR = 3 050 EUR **Kopā 2018.gadā un turpmāk katru gadu: 19 929 EUR (EKK 2235)**
3	Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana	Ieviest rīku, kas nodrošinātu Microsoft operētājsistēmu un citas programmatūras (piemēram, Java, e-parasktītājs, u.c.) drošības ielāpu pārvaldības (uzstādīšanu, noņemšana, izplatīšana) automatizāciju, tādejādi garantējot, ka IeM infrastruktūrā tiek izmantota tikai droša programmatūra ar instalētiem pēdējiem drošības ielāpiem.		Antivīrusa risinājuma abonēšana: Programmatūras drošības ielāpu pārvaldības risinājums serveriem: 60 EUR x 160 licences= 9 600 EUR; Programmatūras drošības ielāpu pārvaldības risinājums datoriem: 16 EUR x 8 100 licences= 129 600 licences **Kopā 2018.gadā: 139 200 EUR** (EKK5121), 2019. gadā un turpmāk **139 200 EUR (EKK 2252)**
4	Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve	Izmantojot modernas piekļuves līmeņa vadāmas tīkla iekārtas, lokālajos tīkos tiks nodrošināta pakāpeniska tīkla līmeņa autentifikācijas sistēmas ieviešana, kas liegs iespēju pie IeM iestāžu lokālajiem tīkliem patvaļīgi pieslēgt neautorizētas iekārtas (datorus, mobilās iekārtas, u.t.m.l.). Pasākuma nodrošināšanai tiks izmantots arī esošais finansējums. **Pilnīga ieviešana paredzēta 4 gadu laikā.** **Infrastruktūras paplašināšana un tīkla līmeņa autentifikācijas ieviešana visās IeM padotības iestādēs visā Latvijas teritorijā iespējama tikai, ieviešot papildu datordrošības struktūrvienību, taču daļēja komutatoru iegāde jau esošo nomaiņai, iespējama 2017.gadā.**	**2017.gadā:** 126 gab.x 6000 EUR = ekspluatācijā esošo komutatoru nomaiņa sakārtotā fiziskā tīkla infrastruktūrā (2400 darba vietām) ar atbalstu uz 3 gadiem = 756 000 EUR (EKK5238) **2018., 2019., 2020. gads** - katru gadu 1700 darba vietu ierīkošana, sakārtojot fiziskā tīkla infrastruktūru: 1700 darba vietām nepieciešami 88 komutatori (1700 x 2,5/48) -Komutatori: 88 gab. x 6000 EUR= 528 000 EUR (EKK5238) -Fiziskā tīkla izbūve: 1700 x 2,5 x 87 EUR =369 750 EUR (EKK2249) Kopā gadā 528 000 +369 750= 897 750 EUR	Kopumā komutatoru dzīves cikls paredzams uz 10 gadiem. Komutatoru aparatūras un programmatūras uzturēšana iekļauta uz 3 gadiem, papildu finansējums uzturēšanai jāparedz 10% apmērā gadā no komutatoru iegādes izmaksām, sākot no 2020. gada. **2020.gadā:** 756 000 EUR x 10% = 75 600 EUR (EKK2243) **2021.gadā:** (528 000 EUR + 756 000 EUR) x 10% = 128 400 EUR (EKK2243) **2022.gadā:** (2 gadi x 528 000 EUR + 756 000 EUR) x 10% = 181 200 EUR (EKK2243) **2023.gadā un turpmāk katru gadu:** (3 gadi x 528 000 EUR + 756 000 EUR) x 10% = 234 000 EUR (EKK2243)

			Kopā 3 gados = 897 750 EUR x 3 = 2 693 250 EUR Kopējās ieviešanas izmaksas = 756 000 EUR + 2 693 250 EUR = 3 449 250 EUR	
5	Priviliģēto kontu pārvaldības risinājums	Nepieciešams, lai pārvaldītu - izolētu un papildus aizsargātu jebkura darbinieka rekvizītus (lietotājvārdus, paroles), kuriem ir priviliģētas tiesības IeM IKT infrastruktūrā, piemēram, datortīklu un datorsistēmu administratorus, u.t.m.l. Risinājums ļautu uzraudzīt un kontrolēt izstrādātāju un uzturētāju, t.sk. ārpakalpojumu sniedzēju, veiktās darbības IeM IKT infrastruktūrā **Iespējams tikai, ieviešot papildu datordrošības struktūrvienību.**	**2018. gadā:** -Licence "PAS Server Infrastructure (Software) Includes Vault Server license, 1 CPM license, 10 user licenses, 200 password licenses and Password Vault web-access Ready for AIM, OPM, PSM and SSH" 1 gab 15 972 EUR (EKK5121) -Licence "Server Disaster Recovery module (Software) Includes full passive support for all services and components of the Production installation" 1 gab. 7 865 EUR (EKK5121) -Licence "Server High Availability module (Software) Includes full passive support for all services and components of the Production installation"1 gab. 7 865 EUR (EKK5121) -Licence "Additional 10 user"1 gab. 5 324 EUR (EKK5121) -Licence "30 PSM concurrent session"1 gab. 56 870 EUR (EKK5121) -Programmatūras uzstādīšanas un konfigurēšanas pakalpojumi 726 EUR x 10 cilvēkdienas = 7 260 EUR (EKK5121) **Kopā 101 156 EUR (EKK 5121)**	Atjauninājumu pakalpojums (1 gadam, 15% no iegādes izmaksām) 101 156 x 15% = 15 174 EUR (EKK 2252) Tehniskais atbalsts (8x5, phone, mail, on-site – klātienes vizītes, provizoriski 10 reizes gadā) 10 gab. x 300 EUR = 3000 EUR (EKK 2259) **Kopā 2019.gadā un turpmāk katru gadu 15 174 EUR+3000 EUR = 18 174 EUR**
6	Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai	Nodrošina datu pārraides tīklu segmentu loģisko atdalīšanu, veicot datu plūsmas kontroli starp tiem, tādejādi radot iespējas ierobežot ļaunatūru izplatību starp tīkla segmentiem. Risinājums nepieļauj neautorizētu informācijas apmaiņu starp datu pārraides tīkla segmentiem, tādejādi nodrošinot papildus aizsardzību.	**2018.gadā:** Datortīkla aizsardzība ar augstās pieejamības risinājuma ugunsmūra iekārtām ir jānodrošina ar 10 pieslēgumiem: 10 punkti x 27 921,96 EUR = 279 219,60 EUR ; un ar augstās veiktspējas ugunsmūra iekārtām vēl 10 pieslēgumiem: 10 punkti x	**2019.gadā un turpmākajos gados:** Ikgadējo tehnisko apkopju veikšana un to laikā nomainīto bojāto rezerves daļu apmaksu vidēji gadā uz vienu datortīkla drošības sistēmu 6 132,28 EUR. Kopējās izmaksas: 20 gab. x 6 132,28 EUR = 122 645,60 EUR. **Kopā katru gadu 122 645,60 EUR (EKK**

		Nepieciešamais finansējuma apjoms iekļauts IeM IC 2018. gada prioritāro pasākumu saraksta 6. pasākumā	15 512,20 EUR = 155 122,00 EUR. Kopējās izmaksas ir: 279 219,60 + 155 122,00 = 434 341,60 EUR. **Kopā 2018.gadā 434 342 EUR** (EKK5238) **2019.gadā:** Nepieciešamo datortīkla drošības sistēmas papildus licenču iegāde: 1. Augstās pieejamības drošības vārtejas – 2 gab. x 30 195,55 = 60 391,10 EUR; (EKK 5238) 2. Virtuālo sistēmu licences – 10 gab. x 2 548,26 = 25 482,60 EUR (EKK 5121); 3. 50 mobilo klientu piekļuves licences – 2 gab. x 3 921,61 EUR = 7 843,22 EUR (EKK 5121); 4.Notikumu korelācijas un atskaišu veidošanas licence – 23 217,48 EUR (EKK 5121). **Kopā 2019.gadā 116 934 EUR** **2020.gadā:** Vidēja ātruma 99 pieslēguma punkti x 2 968,13 EUR = 293 844,87 EUR. Maza ātruma 75 pieslēguma punkti x 1 662,54 EUR = 124 690,50 EUR. **Kopā 2020.gadā 418 536 EUR** (EKK5238) **Kopā 3 gados: 969 811 EUR**	**2243)** **2020.gadā un turpmākajos gados:** Jauninājumu un tehniskā atbalsta abonēšana vienam gadam: 1. augstās pieejamības drošības vārtejas - 2 gab. x 12 577,95= 25 155,90 EUR (EKK2243) 2. virtuālo sistēmu licences - 10 gab. x 370,26 = 3 702,60 EUR (EKK2252); 3.50 mobilo klientu piekļuves licences - 2 gab. x 569,91=1139,82 EUR (EKK252); 4. notikumu korelācijas un atskaišu veidošanas licences atjauninājums - 3 373,48 EUR (EKK2252). **Kopā katru gadu: 33 372 EUR** **Kopā 2019.gadā 122 646 EUR** (*aprēķinu skatīties augstāk)* **Kopā 2020.gadā un turpmākajos gados katru gadu :** **122 645,60 EUR + 33 372 EUR = 156 018 EUR**
7	Vienotas informācijas aizsardzības pārvaldības sistēmas izveidošana Iekšlietu ministrijā un tās	Pasākumu īstenošanas rezultātā tiks izveidota droša tehnoloģiskā vide elektroniskās informācijas apstrādei, tādejādi nodrošinot ierobežotas pieejamības informācijas aizsardzību IeM un tās padotības iestādēs. Risinājums nodrošinās visu lietojumprogrammu darbināšanas vadību (ietverot pretvīrusu aizsardzības	IT drošības sistēmas ieviešana kas paredz 7500 licenču iegādi: 7500 gab x 384 EUR = **2 880 000 EUR**. IT drošības sistēma uzstādāma uz katra datora un tās kopējā cena atkarīga no pārvaldāmo un aizsargājamo datoru skaita.	Ikgadējās tehniskā atbalsta un uzturēšanas izmaksas sastāda 15 % no licenču cenas, t.i. 384 EURx0,15= 57,60 EUR (EKK2252) **2020.gadā:** 2500 licences x 57,60 EUR = 144 000 EUR

	padotības iestādēs (DLP)	funkcionalitāti), ārējo iekārtu (tai skaitā maināmo datu nesēju) pieslēgumu centralizētu pārvaldību un pārraudzību lietotāju darba vietās. **Iespējams tikai, ieviešot papildu datordrošības struktūrvienību, ņemot vērā pasākuma sarežģītību no 2019. gada.**	**2019.,2020., 2021. gadā:** 2500 licences x 384 EUR = 960 000 EUR Kopā 3 gados = **2 880 000 EUR (EKK5121)**	**2021.gadā:** 5000 licences x 57,60 EUR = 288 000 EUR **2022.gadā un turpmākajos gados katru gadu:** 7500 licences x 57,60 EUR = 432 000 EUR
8	Drošības testu veikšana	Lai gūtu pārliecību par ieviesto tehnoloģiju un risinājumu efektivitāti, katru gadu nepieciešams veikt drošības testus. **Iespējams tikai, ieviešot papildu datordrošības struktūrvienību**		Saskaņā ar IUB mājaslapā publicēto vienas informācijas sistēmas (iepirkuma ID: PMLP 2015/20) drošības audits un ielaušanās testa izmaksas ir 11 737 EUR. Atkarībā no drošības testa satura un mēroga, iespējamās izmaksas vairākām informācijas sistēmām tiek prognozētas no 10 000 EUR līdz 30 000 EUR, tātad **vidēji 20 000 EUR gadā (EKK2259).**

3.pielikums

Pasākumu plānoto izdevumu tāmes kopsavilkums sadalījumā pa izdevumu kodiem atbilstoši ekonomiskajām kategorijām (EKK)

A variants

EKK	EKK nosaukums	Izdevumu pamatojums (pasākums)	2017. gads	2018.gads	2019.gads	2020.gads	2021.gads	2022.gads
2	3	4	5	6	7	8	9	10
1000-9000	**Izdevumi-kopā**		**2 933 558**	**4 025 921**	**4 708 177**	**5 262 750**	**4 143 265**	**3 380 065**
1000-2000	**Kārtējie izdevumi**		**444 158**	**1 494 823**	**1 774 843**	**2 027 815**	**1 854 865**	**2 051 665**
1000	**Atlīdzība**		**146 483**	**793 544**	**793 544**	**793 544**	**793 544**	**793 544**
1100	**Atalojums**		**118 523**	**616 394**	**616 394**	**616 394**	**616 394**	**616 394**
1110	Mēnešalga		98 769	513 661	513 661	513 661	513 661	513 661
1119	Pārējo darbinieku mēnešalga (darba alga)	1. **Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 118 584 EUR 2. **IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 98 769 EUR 2018.gads un turpmāk ik gadu 395 077 EUR	98 769	513 661	513 661	513 661	513 661	513 661
1140	Piemaksas, prēmijas un naudas balvas		19 754	102 733	102 733	102 733	102 733	102 733
1147	Piemaksa par papildu darbu	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 11 858 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 9877 EUR 2018.gads un turpmāk ik gadu 39 508 EUR	9 877	51 366	51 366	51 366	51 366	51 366
1148	Prēmijas un naudas balvas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 11 859 EUR **2.IKT personāla atlīdzības konkurētspējas**	9 877	51 367	51 367	51 367	51 367	51 367

		uzlabošana (pasākums 2.2) 2017.gada 3 mēneši 9 877 EUR 2018.gads un turpmāk ik gadu 39 508 EUR						
1200	**Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas, pabalsti un kompensācijas**		**27 960**	**177 150**	**177 150**	**177 150**	**177 150**	**177 150**
1210	Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 34 968 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 27 960 EUR 2018.gads un turpmāk ik gadu 116 499 EUR	27 960	151 467	151 467	151 467	151 467	151 467
1220	Darba devēja pabalsti, kompensācijas un citi maksājumi			25 683	25 683	25 683	25 683	25 683
1221	Darba devēja pabalsti un kompensācijas, no kuriem aprēķina iedzīvotāju ienākuma nodokli un valsts sociālās apdrošināšanas obligātās iemaksas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 5 929 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2018.gads un turpmāk ik gadu 19 754 EUR		25 683	25 683	25 683	25 683	25 683
2000	**Preces un pakalpojumi**		**297 675**	**701 279**	**981 299**	**1 234 271**	**1 061 321**	**1 258 121**
2200	Pakalpojumi		6 075	409 679	689 699	942 671	769 721	966 521
2230	Iestādes administratīvie izdevumi un ar iestādes darbības nodrošināšanu saistītie izdevumi		6 075	19 929	19 929	19 929	19 929	19 929
2235	Izdevumi par saņemtajiem apmācību pakalpojumiem	**Apmācības (pasākums 2.3)** 2017.gads 6 075 EUR 2018.gads un turpmāk ik gadu 19 929 EUR	6 075	19 929	19 929	19 929	19 929	19 929
2240	Remontdarbi un iestāžu uzturēšanas pakalpojumi (izņemot kapitālo remontu)			369 750	492 396	593 152	276 202	329 002

2243	Iekārtas, inventāra un aparatūras remonts, tehniskā apkalpošana	**1.Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve (pasākums 4)** 2020.gads 75 600 EUR 2021.gads 128 400 EUR 2022.gads 181 200 EUR **2. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2019.gads 122 646 EUR 2020.gads un turpmāk ik gadu 147 802 EUR			122 646	223 402	276 202	329 002
2249	Pārējie remonta darbu un iestāžu uzturēšanas pakalpojumi	**1.Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve (pasākums 4)** 2018.gads, 2019.gads, 2020.gads 369 750 EUR ik gadu		369 750	369 750	369 750		
2250	Informācijas tehnoloģijas pakalpojumi			20 000	177 374	329 590	473 590	617 590
2252	Informācijas sistēmas licenču nomas izdevumi	1. **Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana (pasākums 3)** 2019.gads un turpmāk ik gadu 139 200 EUR **2. Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2019.gads un turpmāk ik gadu 15 174 EUR **3. Vienotas informācijas aizsar-dzības pārvaldības sistēmas izvei-došana Iekšlietu ministrijā un tās padotības iestādēs (DLP) (pasākums 7)** 2020.gads 144 000 EUR 2021.gads 288 000 EUR 2022.gads un turpmāk ik gadu 432 000 EUR			154 374	298 374	442 374	586 374
2259	Pārējie informācijas tehnoloģiju pakalpojumi	**1. Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2019.gads un turpmāk ik gadu 3000 EUR **2. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2020.gads un turpmāk ik gadu 8 216 EUR **3. Drošības testu veikšana (pasākums 8)** 2018.gads un turpmāk ik gadu 20 000 EUR		20 000	23 000	31 216	31 216	31 216
2300	Krājumi, materiāli, energoresursi, prece, biroja preces un		291 600	291 600	291 600	291 600	291 600	291 600

	inventārs, kurus neuzskaita kodā 5000							
2310	Izdevumi par precēm iestādes darbības nodrošināšanai		291 600	291 600	291 600	291 600	291 600	291 600
2312	Inventārs	**1. Datortehnikas plānveida nomaiņa (pasākums 1A)** 2017.gads un turpmāk ik gadu 291 600 EUR	291 600	291 600	291 600	291 600	291 600	291 600
5000	**Pamatkapitāla veidošana**		**2 489 400**	**2 531 098**	**2 933 334**	**3 234 935**	**2 288 400**	**1 328 400**
5120	Licences, koncesijas un patenti, preču zīmes un līdzīgas tiesības			240 356	1 106 543	960 000	960 000	
5121	Datorprogrammas	**1. Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauni-nājumu pārvaldības rīka ieviešana (pasākums 3)** 2018.gads 139 200 EUR **2. Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2018.gads 101 156 EUR **3. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2019.gads 56 543 EUR **4. Vienotas informācijas aizsar-dzības pārvaldības sistēmas izvei-došana Iekšlietu ministrijā un tās padotības iestādēs (DLP) (pasākums 7)** 2019.gads, 2020.gads, 2021.gads 960 000 EUR ik gadu		240 356	1 106 543	960 000	960 000	
5200	Pamatlīdzekļi		2 489 400	2 290 742	1 916 791	2 274 935	1 328 400	1 328 400
5230	Pārējie pamatlīdzekļi		2 489 400	2 290 742	1 916 791	2 274 935	1 328 400	1 328 400
5238	Datortehnika, sakaru un cita biroja tehnika	**1.Datortehnikas plānveida nomaiņa (pasākums 1A)** 2017.gads 1 733 400 EUR 2018.gads un turpmāk ik gadu 1 328 400 EUR **2. Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve (pasākums 4)** 2017.gads 756 000 EUR 2018.gads, 2019.gads, 2020.gads 528 000 EUR ik gadu	2 489 400	2 290 742	1 916 791	2 274 935	1 328 400	1 328 400

		3. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6) 2018.gads 434 342 EUR 2019.gads 60 391 EUR 2020.gads 418 535 EUR						

B variants

EKK	EKK nosaukums	Izdevumu pamatojums (pasākums)	2017. gads	2018.gads	2019.gads	2020.gads	2021.gads	2022.gads
2	3	4	5	6	7	8	9	10
1000-9000	**Izdevumi-kopā**		**908 558**	**2 405 921**	**3 088 177**	**8 410 150**	**729 665**	**6 527 465**
1000-2000	**Kārtējie izdevumi**		**152 558**	**1 203 223**	**1 483 243**	**3 069 615**	**2 896 665**	**3 093 465**
1000	**Atlīdzība**		**146 483**	**793 544**	**793 544**	**793 544**	**793 544**	**793 544**
1100	**Atalgojums**		**118 523**	**616 394**	**616 394**	**616 394**	**616 394**	**616 394**
1110	Mēnešalga		98 769	513 661	513 661	513 661	513 661	513 661
1119	Pārējo darbinieku mēnešalga (darba alga)	3. **Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 118 584 EUR 4. **IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 98 769 EUR 2018.gads un turpmāk ik gadu 395 077 EUR	98 769	513 661	513 661	513 661	513 661	513 661
1140	Piemaksas, prēmijas un naudas balvas		19 754	102 733	102 733	102 733	102 733	102 733
1147	Piemaksa par papildu darbu	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 11 858 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 9877 EUR 2018.gads un turpmāk ik gadu 39 508 EUR	9 877	51 366	51 366	51 366	51 366	51 366
1148	Prēmijas un naudas balvas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 11 859 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 9 877 EUR 2018.gads un turpmāk ik gadu 39 508 EUR	9 877	51 367	51 367	51 367	51 367	51 367
1200	**Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas, pabalsti un kompensācijas**		**27 690**	**177 150**	**177 150**	**177 150**	**177 150**	**177 150**

1210	Darba devēja valsts sociālās apdrošināšanas obligātās iemaksas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 34 968 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2017.gada 3 mēneši 27 960 EUR 2018.gads un turpmāk ik gadu 116 499 EUR	27 690	151 467	151 467	151 467	151 467	151 467
1220	Darba devēja pabalsti, kompensācijas un citi maksājumi			25 683	25 683	25 683	25 683	25 683
1221	Darba devēja pabalsti un kompensācijas, no kuriem aprēķina iedzīvotāju ienākuma nodokli un valsts sociālās apdrošināšanas obligātās iemaksas	**1.Datordrošības struktūrvienības izveide (pasākums 2.1.)** 2018.gads un turpmāk ik gadu 6 amata vietas 34 968 EUR **2.IKT personāla atlīdzības konkurētspējas uzlabošana (pasākums 2.2)** 2018.gads un turpmāk ik gadu 19 754 EUR		25 683	25 683	25 683	25 683	25 683
2000	**Preces un pakalpojumi**		**6 075**	**409 679**	**689 699**	**2 276 071**	**2 103 121**	**2 299 921**
2200	Pakalpojumi		6 075	409 679	689 699	2 276 071	2 103 121	2 299 921
2230	Iestādes administratīvie izdevumi un ar iestādes darbības nodrošināšanu saistītie izdevumi		6 075	19 929	19 929	19 929	19 929	19 929
2235	Izdevumi par saņemtajiem apmācību pakalpojumiem	**Apmācības (pasākums 2.3)** 2017.gads 6 075 EUR 2018.gads un turpmāk ik gadu 19 929 EUR	6 075	19 929	19 929	19 929	19 929	19 929
2240	Remontdarbi un iestāžu uzturēšanas pakalpojumi (izņemot kapitālo remontu)			369 750	492 396	593 152	276 202	329 002
2243	Iekārtas, inventāra un aparatūras remonts, tehniskā apkalpošana	**1.Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekļuves sistēmas izbūve (pasākums 4)** 2020.gads 75 600 EUR 2021.gads 128 400 EUR 2022.gads 181 200 EUR **2. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2019.gads 122 646 EUR 2020.gads un turpmāk ik gadu 147 802 EUR			122 646	223 402	276 202	329 002
2249	Pārējie remonta darbu un	**1.Vadāmu tīkla komutatoru iegāde un tīkla līmeņa**		369 750	369 750	369 750		

	iestāžu uzturēšanas pakalpojumi	**piekluves sistēmas izbūve (pasākums 4)** 2018.gads, 2019.gads, 2020.gads 369 750 EUR ik gadu						
2250	Informācijas tehnoloģijas pakalpojumi			20 000	177 374	1 662 990	1 806 990	1 950 990
2252	Informācijas sistēmas licenču nomas izdevumi	1. **Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana (pasākums 1B)** 2020.gads, 2021.gads, 2022.gads 900 000 EUR 2. **Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauninājumu pārvaldības rīka ieviešana (pasākums 3)** 2019.gads un turpmāk ik gadu 139 200 EUR **3. Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2019.gads un turpmāk ik gadu 15 174 EUR **4. Vienotas informācijas aizsar-dzības pārvaldības sistēmas izvei-došana Iekšlietu ministrijā un tās padotības iestādēs (DLP) (pasākums 7)** 2020.gads 144 000 EUR 2021.gads 288 000 EUR 2022.gads un turpmāk ik gadu 432 000 EUR			154 374	1 198 374	1 342 374	1 486 374
2259	Pārējie informācijas tehnoloģiju pakalpojumi	**1. Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana (pasākums 1B)** 2020.gads, 2021.gads, 2022.gads 433 400 EUR **2.Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2019.gads un turpmāk ik gadu 3000 EUR **3. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2020.gads un turpmāk ik gadu 8 216 EUR **4. Drošības testu veikšana (pasākums 8)** 2018.gads un turpmāk ik gadu 20 000 EUR		20 000	23 000	464 616	464 616	464 616
5000	**Pamatkapitāla veidošana**		**756 000**	**1 202 698**	**1 604 934**	**5 340 535**	**4 349 000**	**3 434 000**
5120	Licences, koncesijas un patenti, preču zīmes un līdzīgas tiesības			240 356	1 016 543	2 485 000	2 485 000	1 525 000
5121	Datorprogrammas	**1. Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana (pasākums 1B)** 2020.gads, 2021.gads, 2022.gads 1 525 000 EUR **2. Antivīrusa risinājuma nomaiņa un programmatūras drošības atjauni-nājumu pārvaldības rīka ieviešana (pasākums 3)**		240 356	1 016 543	2 485 000	2 485 000	1 525 000

		2018.gads 139 200 EUR **3. Priviliģēto kontu pārvaldības risinājums (pasākums 5)** 2018.gads 101 156 EUR **4. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2019.gads 56 543 EUR **5. Vienotas informācijas aizsar-dzības pārvaldības sistēmas izvei-došana Iekšlietu ministrijā un tās padotības iestādēs (DLP) (pasākums 7)** 2019.gads, 2020.gads, 2021.gads 960 000 EUR ik gadu						
5200	Pamatlīdzekļi		756 000	962 342	588 391	2 855 535	1 909 000	1 909 000
5230	Pārējie pamatlīdzekļi		756 000	962 342	588 391	2 855 535	1 909 000	1 909 000
5238	Datortehnika, sakaru un cita biroja tehnika	**1. Centralizēti pārvaldītu virtuālās darba vietas risinājumu ieviešana (pasākums 1B)** 2020.gads, 2021.gads, 2022.gads 1 414 000 EUR **2. Vadāmu tīkla komutatoru iegāde un tīkla līmeņa piekluves sistēmas izbūve (pasākums 4)** 2017.gads 756 000 EUR 2018.gads, 2019.gads, 2020.gads 528 000 EUR ik gadu **3. Ugunsmūru ieviešana apakštīklu savstarpējai aizsardzībai (pasākums 6)** 2018.gads 434 342 EUR 2019.gads 60 391 EUR 2020.gads 418 535 EUR	756 000	962 342	588 391	2 855 535	1 909 000	1 909 000