IEROBEŽOTA PIEEJAMĪBA

Vai varam paļauties uz informācijas sistēmu pieejamību un e-pakalpojumu saņemšanu?

Rīga, 2022

Latvijas Republikas
Valsts kontrole

Revīzijas ziņojums

2022. gada 26. jūlijs.

Lietderības revīzija "Vai varam paļauties uz informācijas sistēmu pieejamību un e-pakalpojumu saņemšanu?"

Revīzija veikta, pamatojoties uz Valsts kontroles Revīzijas un metodoloģijas departamenta 2020. gada 9. septembra uzdevumu Nr.2.4.1-38/2020.

Vāka noformējumā izmantota fotogrāfija no tīmekļvietnes *Depositphotos: (https://depositphotos.com/41112943/stock-photo-business-strategy.html)* .

Cienījamais lasītāj!

Mūsu ikdiena nav iedomājama bez informācijas un komunikācijas tehnoloģiju (IKT) izmantošanas. Turpina pieaugt iedzīvotājiem pieejamais e-pakalpojumu apjoms un attiecīgi – pakalpojumu sniegšanā apstrādājamās un uzglabājamās informācijas apjoms. Arī izdevumu apjoms informācijas sistēmu (IS) un ar to saistītās IKT infrastruktūras uzturēšanai un darbībai valsts pārvaldē pēdējo piecu gadu laikā ir pieaudzis no 41 milj. *euro* līdz 64 milj. *euro* gadā.

Atbilstoša IS un ar tām saistītās IKT infrastruktūras darbība ir priekšnosacījums pieejamībai, bez kuras e-pakalpojumu sniegšana nav iespējama.

Iespēju saņemt iestāžu sniegtos pakalpojumus attālinātā veidā (t.sk. e-pakalpojumu veidā) īpaši ir aktualizējusi Covid-19 pandēmija. Izvēloties saņemt e-pakalpojumu, mēs sagaidām, ka tas būs pieejams šīs izvēles izdarīšanas brīdī. Jebkuri šķēršļi saņemt e-pakalpojumu izvēlētajā brīdī rada izmaksas – gan e-pakalpojuma saņēmējam, gan arī e-pakalpojumu sniedzošai iestādei. Bet cik lielas ir šīs izmaksas un kuros gadījumos tās ir attaisnojamas – šādas aplēses tā īsti neviens nav veicis.

Šajā lietderības revīzijā mēs meklējām atbildi uz jautājumu – *vai varam paļauties uz IS pieejamību un e-pakalpojumu saņemšanu*? Tomēr viennozīmīgu atbildi tā arī neguvām – iestāžu sniegtā informācija par IS un e-pakalpojumu pieejamības līmeni lielākoties ir viedokļos, nevis faktos balstīta, jo nav skaidrības, kā pieejamību izmērīt – nav aprēķina metodikas un netiek uzkrāti rādītāji, lai to mērītu. Arī valstiskā līmenī informācija par sasniegto IS un e-pakalpojumu pieejamības līmeni apkopota netiek.

Atbildība par iestāžu IS uzturēšanu un drošību, kā arī IS darbības nepārtrauktību ir noteikta iestādei, tomēr e-pakalpojumu pieejamības nodrošināšanā nereti iesaistītas ir arī citu iestāžu uzturētās IS. Tādējādi, lai pakalpojumu saņēmējs varētu garantēti saņemt e-pakalpojumu, vienlaicīgi pareizi ir jāstrādā ne tikai visām savstarpēji saistītajām IS, bet arī IKT infrastruktūrai un sakaru kanāliem. Šis ir izaicinājums iestādēm, ko ne vienmēr izdodas realizēt.

Lai gan valstiskā līmenī ir apzināts IS pieejamības nozīmīgums (t.sk. e-pakalpojumu nodrošināšanai) un iestādēm normatīvajos aktos ir izvirzīti ieviešamie priekšnoteikumi IKT darbības nepārtrauktības organizēšanai un IS (t.sk. e-pakalpojumu) pieejamības nodrošināšanai, tomēr iestādes nesteidz tos ieviest un pārliecināties, vai tādejādi tiek nodrošināta IKT darbības nepārtrauktība, IS un e-pakalpojumu pieejamība, un vai incidenta gadījumā ir panākama IS pieejamības atjaunošana iespējami īsā laikā.

Revīzijas noslēgumā esam formulējuši un saskaņojuši vairākus ieteikumus, tāpēc pateicamies par sadarbību gan Vides aizsardzības un reģionālās attīstības ministrijai, gan Aizsardzības ministrijai un iestādēm, kas sniedza revīzijai nepieciešamo informāciju, lai novērtētu situāciju IKT darbības nepārtrauktības organizēšanā un IS (t.sk. e-pakalpojumu) pieejamības nodrošināšanā.

ar cieņu
departamenta direktore

Ilze Bādere

Saturs

Kopsavilkums

Galvenie secinājumi

Vidēji valsts pārvalde tērē 51 milj. *euro* gadā[1] informācijas tehnoloģiju pakalpojumiem. Tie ir izdevumi, lai nodrošinātu informācijas sistēmu (turpmāk – IS) un ar to saistītās informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) infrastruktūras uzturēšanu un darbību, bet ne to attīstības izdevumus. IS atbilstoša darbība ir pamats e-pakalpojumu un to atbalstošo IS pieejamībai, savukārt iestāžu sasniegtais IS pieejamības līmenis ir viens no IS uzturēšanas izmaksu efektivitātes rādītājiem.

Revīzijā konstatētas problēmas ne tikai sasniegtās IS pieejamības novērtēšanā, bet arī IS pieejamības pārvaldībā kopumā, līdz ar ko **revidenti nevar sniegt atbildi uz jautājumu "*Vai varam paļauties uz IS pieejamību un e-pakalpojumu saņemšanu?*", jo revīzijā to viennozīmīgi noteikt neizdevās** šādu iemeslu dēļ:

- vienkopus netiek uzkrāta un analizēta informācija par sasniegto e-pakalpojumu un to atbalstošo IS pieejamības līmeni. Arī tā informācija, kas ir atsevišķu vadošo e-pārvaldes un IS drošības jomas iestāžu – VARAM par valsts IS un tehniskajiem resursiem, CERT.LV par IT drošības incidentiem, VRAA par e-pakalpojumu darbības traucējumiem un nepieejamību portālā Latvija.lv – rīcībā, vienkopus analizēta netiek;
- nav skaidrs, ko mērīt, kādā veidā un nav arī aprēķina metodikas. Iestādes sasniegto IS pieejamību izprot dažādi – nemēra neko un pat neizvirza IS pieejamību kā nepieciešamību, mēra tikai datu bāzu pieejamību (kas ir viena no komponentēm, lai IS un e-pakalpojums darbotos), dažādi interpretē IS drošības incidentus;
- pastāv trūkumi arī attīstības plānošanas jomā, jo nav noteikta nepieciešamība apzināt un vērtēt situāciju e-pakalpojumu un to atbalstošo IS pieejamībā. Arī attiecībā uz valsts pārvaldes sniegto pakalpojumu kvalitāti e-pakalpojuma pieejamība nav izvirzīta kā kvalitātes rādītājs;
- nav skaidrs, kā nodrošināt un ko uzraudzīt, lai sasniegtu normatīvajos aktos noteikto pieejamības līmeni – integrētajām valsts IS (98%), savietotājam (99%) un e-pakalpojumiem (98%). Turklāt arī normatīvajos aktos izvirzītie organizatoriskie priekšnoteikumi IS pieejamības nodrošināšanai un darbības nepārtrauktības atjaunošanai iestādēs nav pilnībā ieviesti;
- netiek salāgots IS izvirzītais darbības laiks un sasniedzamais pieejamības līmenis starp visām e-pakalpojuma nodrošināšanā iesaistītajām komponentēm – atbalstošo IS, IKT infrastruktūru, integrētajām IS un arī attiecībā uz vietu, kur e-pakalpojums ir izmitināts (iestādes tīmekļvietne vai portāls Latvija.lv);
- nav noteikts, kāds ir e-pakalpojuma darba laiks, t.i., vai var sagaidīt e-pakalpojuma pieejamību iestādes darba laikā vai 24/7 darbības režīmā.

Par to, ka IS un e-pakalpojumu pieejamības pārvaldībā ir risināmas problēmas, liecina daudzi e-pakalpojumu darbības traucējumu un nepieejamības gadījumi. Saskaņā ar revidentu novērojumiem portālā Latvija.lv no 2022.gada janvāra līdz martam ar e-pakalpojumu pieejamības traucējumiem varēja saskarties vismaz 84 tūkst. potenciālo e-pakalpojumu lietotāju (tika novērotas tehniskas problēmas, kā rezultātā e-pakalpojums varēja nenotikt), no tiem 10 000 gadījumos e-pakalpojumu pieprasīt nevarēja vispār. Arī saskaņā ar VRAA, kas nodrošina portāla Latvija.lv darbību, sniegto

informāciju novēroto kļūdu skaits e-pakalpojumu izsaukumos atsevišķiem – nestabilākajiem pakalpojumiem, mēdz sasniegt 40–60%. Tādējādi secināms, ka faktiskais e-pakalpojumu saņēmēju skaits, kas sastopas ar e-pakalpojumu darbības traucējumiem vai to nepieejamību, varētu būt lielāks nekā revidentu aplēsē aprēķinātais (balstoties uz e-pakalpojumu izmantošanas statistiku 2020.gadā).

Latvijā līdz šim nav veiktas aplēses, cik daudz ir izmaksājusi IS nepieejamība un kādas sekas tas ir radījis privātpersonām vai plašāk – tautsaimniecībai. Revidentu ieskatā sekas IS un e-pakalpojumu nepieejamībai varētu būt ievērojamas, jo, piemēram, saskaņā ar CERT.LV apkopoto informāciju[2] par IS drošības incidentiem valsts pārvaldē vienā no incidentiem vien tika ietekmēta [IP] valsts un pašvaldību iestāžu vietņu darbība. Savukārt e-pakalpojuma nepieejamība rada sekas gan pakalpojumu saņēmējam, kuram ir jāmeklē alternatīvs risinājums pakalpojuma saņemšanai vai jātērē laiks, pārbaudot, vai pakalpojuma pieejamība ir atjaunota, gan arī valsts pārvaldei, apkalpojot privātpersonu mazāk automatizētā pakalpojumu sniegšanas kanālā. Saskaņā ar revīzijā veikto aplēsi (2.tabula) e-pakalpojuma saņemšana citā, nevis attālinātā veidā pakalpojuma saņēmējam var radīt izmaksas 15,40 *euro* un var nākties patērēt vidēji 1,5 stundu laika, lai to saņemtu klātienē. Pakalpojuma nepieejamības gadījumā arī iestādes ir spiestas tērēt resursus (1,83 *euro* apmērā par vienu pakalpojumu), ko tās varētu izmantot citu, mazāk automatizētu funkciju nodrošināšanai.

Turklāt IS nepieejamības gadījumā sekas varēja rasties ne tikai pašai iestādei, bet arī citām iestādēm, kuras savlaicīgi nesaņēma nepieciešamo informāciju un nevarēja sniegt pakalpojumus.

Prasība nodrošināt pieejamību pati par sevi pieejamību nenodrošina. Ir jāveido ne tikai atbilstoša iekšējās kontroles vide, jāievieš IS drošības un IKT pārvaldība, bet arī jāmēra sasniegtais rezultāts. Revīzijā tika atklāts, ka šajā jomā joprojām ir gan problēmas, gan arī daudz jautājumu par to, kā pieejamību pareizi organizēt, secinot, ka kopumā e-pakalpojumu un to atbalstošo IS pieejamība netiek labi pārvaldīta un uzraudzīta. Turklāt šai rīcībai jābūt savstarpēji koordinētai starp iestādēm, jo ļoti bieži, lai e-pakalpojums darbotos, tā izpildē ir iesaistītas vairākas iestādes un to uzturētās IS. Tas nozīmē, ka visiem šiem komponentiem ir jābūt pieejamiem un pat vienas komponentes darbības traucējumi ietekmēs e-pakalpojuma saņemšanu. Piemēram, lai iedzīvotājs saņemtu e-pakalpojumu portālā Latvija.lv, nepieciešams, lai darbotos:

- portāls Latvija.lv, kuru uztur VRAA;
- lietotāja autentifikācijas mehānisms, kuru nodrošina LVRTC vai kāda no komercbankām;
- pati IS un e-pakalpojumu izpildošie servisi, kurus uztur iestāde;
- saistītās IS un servisi, kas nepieciešami, piemēram, personas datu pārbaudei Iedzīvotāju reģistrā, kuru uztur PMLP;
- datu apmaiņas kanāli, kurus uztur dažādi telekomunikāciju pakalpojumu sniedzēji;
- savietotājs, kuru uztur VRAA.

Prasība sasniedzamajam e-pakalpojumu pieejamības līmenim ir noteikta, bet mehānisms tās izpildes uzraudzībai nav ieviests

Lai gan prasības sasniedzamajam pieejamības līmenim integrētajām valsts IS un savietotājam ir izvirzītas kopš 2012. gada, e-pakalpojumiem – kopš 2017. gada, un valsts attīstības plānošanas dokumentos tiek uzsvērta IS un e-pakalpojumu pieejamības nepieciešamība, tomēr valsts pārvaldē nav veikta analīze, kāds ir faktiski sasniegtais e-pakalpojumu un to atbalstošo IS pieejamības līmenis. Nav arī noteikta atbildīgā iestāde, kurai šādas informācijas apkopošana un analīze būtu jāveic. To neparedz normatīvie akti nedz IT drošības jomā, nedz valsts pārvaldes pakalpojumu jomā. Lai gan viens no valsts pārvaldes principiem ir, ka valsts pārvalde savā darbībā pastāvīgi pārbauda un uzlabo sabiedrībai sniegto pakalpojumu kvalitāti, un ir noteikti rādītāji, kas jāmēra un jāpublicē Pakalpojumu sniegšanas un pārvaldības platformā, tomēr tie neietver e-pakalpojuma pieejamības rādītājus, kas revidentu ieskatā ir viens no būtiskākajiem pakalpojuma kvalitātes rādītājiem. Līdz ar to tas, vai iestāde nodrošina vai nenodrošina e-pakalpojumus un to atbalstošo IS darbību, ir tikai iestādes darba kārtības jautājums.

Valstī nav vērtēts, vai e-pakalpojumu un to atbalstošo IS pieejamības līmenis ir sasniegts

Lielākā daļa no deviņām revīzijas apjomā iekļautajām iestādēm atzīst, ka to rīcībā nav ne datu, ne rīku, ar kuru palīdzību uzraudzīt un mērīt IS un e-pakalpojumu pieejamību, kā arī nav metodikas, pēc kuras veikt e-pakalpojumu un to atbalstošo IS pieejamības aprēķinu.

Tikai trīs no revīzijas apjomā iekļautajām iestādēm ir mērījušas faktiski sasniegto pieejamības līmeni e-pakalpojumiem vai savām uzturētajām IS. Pārējās sešas iestādes norāda, ka to uzturētās IS ir strādājušas ar augstu pieejamības līmeni, to pamatojot nevis ar datiem, bet ar to, ka nav novēroti būtiski IKT drošības incidenti, kas būtu ietekmējuši IS pieejamību.

Iestādēs trūkst gan metodikas, gan datu, lai noteiktu sasniegto e-pakalpojumu un to atbalstošo IS pieejamības līmeni.

Vienlaikus sešas no deviņām revīzijas apjomā iekļautajām iestādēm ir norādījušas, ka var būt gadījumi, kad pārtraukumi e-pakalpojuma darbībā netiek fiksēti un reģistrēti incidentu reģistrā, savukārt tikai trīs iestādēs ir ieviesta prakse, ka incidentu reģistrā vai kādā citā atsevišķā reģistrā tiek uzkrāta informācija par visiem plānotajiem tehnisko darbu datumiem un pārtraukumu ilgumiem, līdz ar to reģistri nesniedz pilnīgu informāciju par plānotajiem un neplānotajiem e-pakalpojumu un tos atbalstošo IS darbības traucējumiem vai pārrāvumiem un to ilgumu.

Attiecībā uz portālā Latvija.lv izmitināto e-pakalpojumu pieejamību revidenti veica analīzi[3] un konstatēja, ka par 21 e-pakalpojumu publicēti paziņojumi, ka e-pakalpojums nedarbojas. No tiem astoņi e-pakalpojumi nedarbojās no vienas līdz 23 dienām. Tādējādi secināms, ka tie konkrētajā mēnesī ir bijuši pieejami robežās no 26% līdz 96,8%, kas ir mazāk nekā normatīvajā aktā noteiktais 98% sasniedzamais e-pakalpojuma līmenis.

Nacionālā līmenī informāciju par iestādēs notikušajiem IT drošības incidentiem uzkrāj CERT.LV, tomēr ne par visiem notikušajiem incidentiem CERT.LV ir informēta, jo iestādēs nav vienotas pieejas, kad informācija CERT.LV ir jāsniedz.

Arī no CERT.LV pārskatos uzrādītās informācijas revidenti nevarēja gūt visaptverošu priekšstatu par faktisko IT drošības incidentu skaitu un ietekmētajām iestādēm, jo informācija pārskatos tiek atspoguļota atšķirīgā griezumā - pārskatos tiek iekļauta informācija par ietekmētajām IP adresēm, un tikai atsevišķos gadījumos tiek apskatīta situācija (IT drošības incidenti) konkrētās iestādēs. Aizsardzības ministrijai iesniegtajos ierobežotas pieejamības pārskatos [IP] incidentu valsts pārvaldes iestādēs, pašvaldībās vai valsts kapitālsabiedrībās ir saistīti ar pakalpojuma pieejamības traucējumiem.

Lai gan atsevišķi informācijas vienumi, kas attiecas uz IS pieejamību, valsts pārvaldē tiek uzkrāti (CERT.LV par IT drošības incidentiem, VRAA par latvija.lv izmitināto e-pakalpojumu pieejamību), centralizētā veidā valstī nav apkopota informācija par problēmām pieejamības līmeņa nodrošināšanā, kā arī nav analizēti problēmu cēloņi un sekas tam, ka noteiktais pieejamības līmenis netiek sasniegts. Ja netiek reģistrētas visas identificētās problēmas un vērtēti to cēloņi, nav iespējams sniegt pamatotus priekšlikumus uzlabojumiem, līdz ar to ilgtermiņā iestādes turpina uzturēt e-pakalpojumus, bet nekas neveicina to pieejamības uzlabošanu.

Priekšnoteikumi e-pakalpojumu un tos atbalstošo IS pieejamības nodrošināšanai iestādēs nav ieviesti

Normatīvajā aktā[4] (t.sk. labajā praksē[5]) ir ietverti priekšnoteikumi, kuru izpilde ir nepieciešama, lai iestādēs sekmētu IS pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktību. Lai gan visās deviņās revīzijas apjomā iekļautajās iestādēs tiek uzturētas paaugstinātas drošības IS, nevienā no tām nav ieviesti visi priekšnoteikumi pilnībā. Biežākās problēmas ir saistītas ar to, ka iestādes (trīs iestādēs) plānošanas dokumentos nav iestrādāts mērķis IS pieejamības nodrošināšanai. Neizvirzot mērķus un uzdevumus IS pieejamības nodrošināšanai, IS pieejamība nav noteikta kā būtiska nepieciešamība iestādes funkciju nodrošināšanai.

Lai gan no revīzijas apjomā iekļautajām iestādēm piecās ir apzināti IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas ir būtiski iestādes funkciju izpildes atbalsta nodrošināšanā, tomēr pārējās četrās iestādēs būtiskie IKT resursi ir identificēti daļēji, piemēram, identificējot tikai IS. Tādējādi visas izrietošās nepārtrauktības plānošanas darbības ir orientētas tikai uz IS darbības nepārtrauktības plānošanu, kas ir tikai daļa no darbības nodrošināšanā iesaistītajiem IKT resursiem. Turklāt incidentu gadījumā (IKT infrastruktūras vai sakaru pakalpojumu bojājuma gadījumā) iestāde nespēs pietiekami ātri reaģēt un novērst problēmas ar IS nesaistītos resursos.

Revidenti izvērtēja priekšnoteikumus, ko revīzijas apjomā iekļautās iestādes paredz līgumos, nododot IS uzturēšanā ārpakalpojuma sniedzējam, un konstatēja, ka IS pieejamības prasības ir vispārīgas un neizvirza sasniedzamo IS pieejamības līmeni. Tas savukārt rada risku, ka normatīvajā aktā noteiktais IS pieejamības līmenis ārpakalpojumā nodotajām IS netiks sasniegts un ārpakalpojumā nodotās sistēmas neveicinās valsts pārvaldē kopumā noteiktā pieejamības līmeņa sasniegšanu.

No tām sešām revīzijā vērtētajām iestādēm, kuras bija izstrādājušas IS atjaunošanas plānu, trijās nav veiktas plāna atbilstības pārbaudes IS pieejamības atjaunošanai, kas samazinātu risku, ka incidentu gadījumā nevarēs nodrošināt IKT darbības un IS pieejamības atjaunošanu pietiekami īsā laikā vai vispār. Iestādēs izstrādātie IS darbības atjaunošanas plāni nav testēti, pārbaudot to pilnīgumu, proti, iestādes nav pārliecinājušās, vai saskaņā ar plānu, pieejamiem tehniskajiem resursiem, uzglabātajām rezerves kopijām un darbinieku kompetenci IS pieejamība ir atjaunojama iestādē noteiktajā laikā.

Iestādes nav pārliecinājušās, vai un kādā laikā to IS pieejamība ir atjaunojama incidenta gadījumā.

Iestādes galvenokārt paļaujas uz rezerves kopiju veidošanai iebūvētajām kontrolēm, kuras rezerves kopiju izveides brīdī ziņo, vai kopija izveidota un vai tā ir izveidota bez kļūdām. Datu atjaunošanas pārbaudi no rezerves kopijas rezerves kopēšanas sistēma neveic, līdz ar to iestāžu paļaušanās tikai uz rezerves kopēšanas sistēmas ziņojumiem par kopijas izgatavošanas faktu un faktiska IS datu atjaunošanas pārbaudes neveikšana ir pretrunā normatīvajā aktā[6] noteiktajam, ka integrētajām valsts IS testa vidē ne retāk kā reizi kalendāra gadā ir jāveic pēdējās pilnās rezerves kopijas un tai sekojošo pieauguma kopiju atjaunošanas pārbaudes.

Attīstības plānošanas jomā nav identificējams ietvars IS pieejamības nodrošināšanai

Lai gan attīstības plānošanas dokumentos[7] ir apzināts IS pieejamības nozīmīgums valstiskā līmenī, t.sk. e-pakalpojumu sniegšanai, tomēr, izņemot vienu sasniedzamo rezultātu "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam", kopumā attīstības plānošanas dokumentos nav noteikti konkrēti sasniedzamie mērķi un uzdevumi IS pieejamības nodrošināšanai un nav izvirzīti rezultatīvie rādītāji, pēc kuriem mērīt un novērtēt sasniegto IS pieejamību.

"Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" ir noteikts sasniedzamais rezultāts un rezultatīvais rādītājs, kas saistāms ar IKT darbības nepārtrauktības nodrošināšanu un IS pieejamību. Rādītājs paredz, ka 85% no visām paaugstinātas drošības līmeņa sistēmām un platformām ir droši rezervētas un atjaunojamas. Tomēr šī rādītāja sasniegšanai nav izvirzīti konkrēti uzdevumi un nedz VARAM (kā politikas plānošanas dokumenta sagatavotājai), nedz AiM (kā vadošajai iestādei IS drošības politikas jomā) vēl 2022.gada sākumā nebija skaidrs, kurš un kādā veidā nodrošinās, kā arī uzraudzīs un mērīs izvirzītā politikas rezultāta sasniegšanu.

Tādējādi attīstības plānošanas dokumentos nav identificējams rīcības ietvars IS pieejamības nodrošināšanā un valsts pārvaldē nav vienotas izpratnes par sasniedzamo IS pieejamības jomā un netiek veiktas mērķtiecīgas darbības, lai to sasniegtu.

Revidentu ieskatā, lai valstiskā līmenī identificētu rīcības ietvaru IS pieejamības nodrošināšanai jeb lai identificētu tās IS, kurām jānodrošina normatīvajos aktos noteiktie pieejamības līmeņi, būtu jāanalizē valsts IS un IKT resursu uzskaites sistēmā (VIRSIS) uzkrātie dati, tomēr arī šajā IS uzskaitītie dati ir nepilnīgi.

Uzkrātie dati par valsts IS un IKT resursiem ir nepilnīgi

VIRSIS ir izstrādāta un ir ieviesta kopš 01.01.2020., tomēr tajā iestādes ir reģistrējušas datus tikai par 127 no 181 valsts IS, kas bija reģistrēta iepriekš uzturētajā "Valsts informācijas sistēmu reģistrā" (turpmāk – VISR). Par lielāko daļu IS (123 IS) to pārziņi ir norādījuši, ka IS paredzētas iestādes iekšējo vajadzību nodrošināšanai, tātad nenodrošina datu apmaiņu ar citām sistēmām vai pakalpojumu sniegšanu, kas liek domāt, ka sistēmas nav korekti klasificētas.

VIRSIS nav uzkrāti dati, kas varētu liecināt par IS datu apmaiņu ar citām IS un to, vai IS ir integrētā valsts IS, kas ir būtiski, lai konstatētu, vai IS ietekmē citas IS. Kvalitatīvu uzskaites datu trūkums neļauj identificēt tādas IS, kurām jānodrošina augstāks pieejamības līmenis, nekā to nosaka nacionālie normatīvie akti, un kurām būtu jāplāno papildu pasākumi un finansējums atbilstoša pieejamības līmeņa nodrošināšanai – piemēram, tām nacionālā līmeņa IS, kas apmainās ar datiem ar citu valstu IS un kurām sasniedzamo IS pieejamības līmeni, kas ir augstāks nekā Latvijas normatīvajos aktos noteiktais, ir noteikusi ES/EEZ.

Revidentu ieskatā trūkumi informācijas uzskaitē ietekmē VARAM spēju sekmīgi plānot vienotu valsts politiku IS un to darbībai nepieciešamo IKT resursu un pakalpojumu attīstībai un uzturēšanai, kā arī nodrošināt uz pierādījumiem balstītas rīcībpolitikas iedibināšanu IKT pārvaldības jomā. Pēc revidentu domām atbilstoša un pietiekama informācija par valsts IS un ar tām saistīto IKT infrastruktūru ir priekšnoteikums vienotu IS pieejamības un IKT darbības nepārtrauktības pārvaldības principu plānošanai, noteikšanai un uzraudzībai.

Vienlaicīgi ar rīcības ietvara identificēšanu IS pieejamības nodrošināšanai valstiskā līmenī ir nepieciešams pārskatīt arī nacionālā līmeņa normatīvajos aktos noteiktās prasības IS un e-pakalpojumu pieejamības līmeņa sasniegšanai, tās salāgojot savā starpā. Revīzijā konstatēti gadījumi, kad integrēto valsts IS darbību regulējošajos normatīvajos aktos IS vidējie pieejamības rādītāji ir noteikti zemāki nekā tie ir noteikti MK noteikumos, kas nosaka pamata prasību IS pieejamības nodrošināšanai, piemēram, IS jānodrošina vidējā pieejamība 97,47% gadā, lai gan kā pamata prasība ir noteikta, ka pieejamība jānodrošina 98% gadā no sistēmai noteiktā darbības laika.

Nesaskaņoto prasību e-pakalpojumu un portāla Latvija.lv pieejamībai dēļ, kopš 2017.gada, iespējams, ir radīts administratīvais slogs 3,84 miljoni *euro* apmērā

Līdzīga situācija ir konstatēta arī saistībā ar e-pakalpojumu izmitināšanu, jo, izmitinot e-pakalpojumu portālā Latvija.lv, tā pieejamība ir iespējama vienīgi portāla Latvija.lv uzturētāja VRAA noteiktajos un nodrošinātajos pieejamības laikos. Ņemot vērā, ka portāla pieejamība saskaņā ar normatīvo aktu prasībām ir jānodrošina vidēji 97,49% gadā, tiek radīts risks, ka iestādes, izmitinot e-pakalpojumus portālā Latvija.lv, nenodrošinās e-pakalpojumiem

noteikto sasniedzamo pieejamības līmeni (98% mēnesī). Saskaņā ar revidenta aprēķiniem tas nozīmē, ka iestādes e-pakalpojums var tikt nodrošināts par gandrīz četrām stundām mēnesī mazākā apjomā, nekā paredz vispārējais regulējums e-pakalpojuma pieejamībai. Šis apstāklis rada risku, ka nesaskaņotu normatīvo aktu prasību dēļ iespējams katru mēnesi valstiski var tikt radīts administratīvais slogs līdz pat 64 tūkst. *euro*[8]. Tā kā normatīvais regulējums, kas nosaka prasības e-pakalpojumu un portāla Latvija.lv pieejamībai ir spēkā kopš 2017.gada, secināms, ka piecu gadu laikā, iespējams, kopumā ir radīts administratīvais slogs 3,84 milj. *euro* apmērā, kurus iedzīvotāji vai valsts pārvalde varēja izmantot citādāk.

Būtiskākie ieteikumi

Pamatojoties uz revīzijas secinājumiem, VARAM un AiM sadarbībā ar CERT.LV sniegti ieteikumi e-pakalpojumu un tos atbalstošo IS pieejamības uzlabošanai:

- VARAM veikt VIRSIS sistēmā uzskaitīto datu kvalitātes pārbaudi un izstrādāt metodiku e-pakalpojumu un to atbalstošo IS sasniegtās pieejamības aprēķināšanai, kā arī veikt darbības, lai veicinātu "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" noteiktā rādītāja – 85% paaugstinātas drošības IS ir atjaunojamas – sasniegšanu;
- AiM un VARAM izstrādāt datu apmaiņas mehānismu un vienotu informācijas uzkrāšanas punktu, lai operatīvi atklātu informāciju par ietekmētajām IS un e-pakalpojumiem un ilgtermiņā sniegtu informāciju par dīkstāves laiku;
- VARAM apkopot informāciju par sasniegto e-pakalpojumu un to atbalstošo IS pieejamības līmeni un veikt IS un e-pakalpojumu nepieejamības seku analīzi;
- VARAM normatīvajos aktos saskaņot prasības e-pakalpojumu un portāla Latvija.lv sasniedzamajam pieejamības līmenim, tostarp darbības laiku;
- AiM sadarbībā ar CERT.LV noteikt ieteicamo par IT drošības incidentu iesniedzamo informācijas apjomu un struktūru;
- valsts pārvaldes elektroniskās telpas uzraudzības pilnveidošanai - AiM sadarbībā ar CERT.LV izstrādāt kritērijus, lai apzinātu iestādes, kurās obligāti ir jāizvieto CERT.LV drošības sensori un sadarbībā ar VARAM izstrādāt stratēģiju drošības sensoru plašākai uzstādīšanai un izmantošanai.

Ziņojuma struktūra

Informācija ziņojumā izklāstīta šādā secībā:

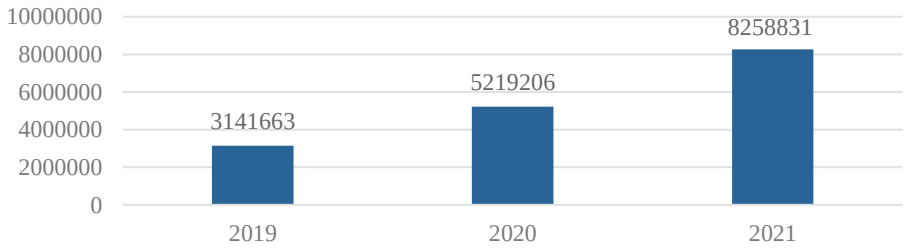
- revīzijas secinājumi, konstatējumi un ieteikumi par revīzijas apjomā ietvertajām jomām – sasniegtais IS un e-pakalpojumu pieejamības līmenis iestādēs, normatīvajos aktos ietvertās prasības IS un e-pakalpojumu pieejamības nodrošināšanai, priekšnoteikumu izpilde iestādēs, lai nodrošinātu IKT darbības nepārtrauktību un IS pieejamību, iestāžu spēja nodrošināt IS pieejamības atjaunošanu incidentu gadījumos, kā arī politikas plānošanu IS un e-pakalpojumu pieejamības nodrošināšanai;
- revidējamo vienību sniegtie viedokļi par veikto revīziju;
- revīzijas raksturojums, kritēriji un metodes (mērķis, juridiskais pamatojums, atbildība, apjoms, ierobežojumi, vērtēšanas kritēriji).

Vai e-pakalpojumu pieejamība ir būtiska, kā to nodrošināt un kurš par to atbild?

Ikdiena nav iedomājama bez IKT izmantošanas. Pakalpojuma sniedzēji, īstenojot valsts pārvaldes funkcijas saskaņā ar normatīvajiem aktiem vai deleģētiem valsts pārvaldes uzdevumiem, var nodrošināt dažādu pakalpojumu sniegšanu iedzīvotājiem[9] un veikt citas tās funkcijas.

Pakalpojumu pieejamības uzlabošanai iestādes piedāvā e-pakalpojumus, kuru darbībai ir svarīga IS un citu iestāžu uzturētu datu pieejamība. Lai nodrošinātu, ka IS un ar to saistītā IKT infrastruktūra ir pieejama, valsts pārvalde vidēji tērē 51 milj. *euro* gadā[10] informācijas tehnoloģiju pakalpojumiem, kas nodrošina IS un ar to saistītās IKT infrastruktūras uzturēšanu un darbību.

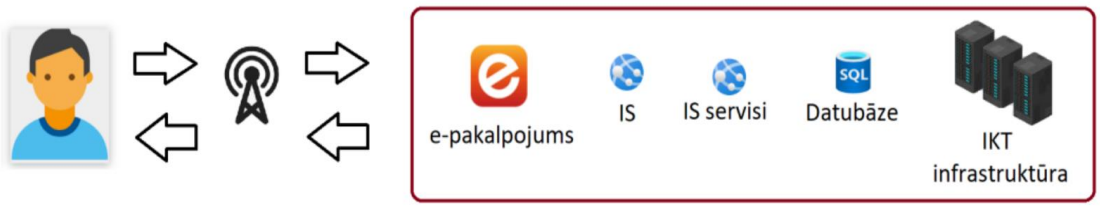
Saskaņā ar Pakalpojumu sniegšanas un pārvaldības platformā pieejamiem datiem par 2020. gadu e-pakalpojumu izmantošanas statistika ir četras reizes augstāka nekā, piemēram, klātienes pakalpojumu izmantošana. Privātpersonu ieradumu maiņu intensīvāk izmantot e-pakalpojumus ir veicinājusi Covid-19 situācija, veicinot to, ka būtisks pakalpojumu īpatsvars tiek izmantots elektroniskā vidē, un attiecīgi ikviens sagaida pakalpojuma pieejamību tajā brīdī, kad izvēlas to saņemt – savukārt, apzinot šāda veida pakalpojumu priekšrocības, visticamāk, arī turpmāk e-pakalpojumu izmantošanas intensitāte saglabāsies (1.attēls).



1.attēls. E-pakalpojumu pieprasīšanas reižu skaits portālā Latvija.lv.

Lietotājs, pieprasot e-pakalpojumu, to saņem atbilstoši gaidītajam vai arī saskaras ar tā darbības traucējumiem vai pat nesaņem vispār. E-pakalpojuma nodrošināšanai ir virkne būtisku komponenšu, kas katra pati par sevi var ietekmēt rezultātu, t.i., to, vai e-pakalpojums strādā vai nestrādā. Turklāt tas ietekmē arī citu iestāžu funkciju izpildi, to starp e-pakalpojumu sniegšanu, ņemot vērā, ka IS var būt integrēta ar citām IS un viena IS var tikt izmantota vairāku e-pakalpojumu nodrošināšanā.

Faktiski "pieejamība" nozīmē, ka lietotājam vajadzīgajā laikā nepieciešamo darbību veikšanai tiek nodrošināta savlaicīga, garantēta piekļuve informācijai, kuras nodrošināšanai ir pieejama IKT infrastruktūra, IS, lietojumprogrammas (t.sk. izveidotie interfeisi, piemēram, e-pakalpojumi) un sakaru tīkli[11] (2.attēls).



2.attēls. E-pakalpojumu sniegšanā iesaistītie informācijas un tehniskie resursi.

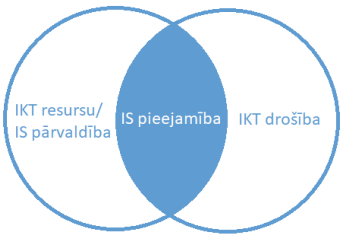
Pakalpojumu nodrošināšanai var būt nepieciešami dati, kuri tiek uzkrāti arī citu iestāžu IS. Šim mērķim starp IS tiek veidota datu apmaiņa un nodrošināta IS integrācija (šādas IS sauc par integrētām IS). Līdz ar to vienas iestādes IS nepieejamība ietekmē ne tikai pašas iestādes funkciju izpildi, bet arī funkciju nodrošināšanu citās iestādēs. Tas jāņem vērā, un iestādēm savstarpēji jāsalāgo sasniedzamie pieejamības līmeņi – ja kādai no iesaistītajām IS vai citas iestādes uzturētai IS tiek noteikts zemāks sasniedzamais pieejamības līmenis, tas var ietekmēt augstāk izvirzīta rādītāja sasniegšanu citai IS.

Normatīvajā aktā[12] sasniedzamais pieejamības līmenis ir noteikts tikai integrētajām valsts IS – 98% gadā no sistēmai noteiktā darbības laika un savietotājam, kas nodrošina centralizētu datu apmaiņas punktu starp valsts IS – 99%. Vienlaikus normatīvais akts[13] nosaka skaidru sasniedzamo pieejamības rādītāju, ja iestāde uztur e-pakalpojumu - iestādei ir jānodrošina e-pakalpojuma darbspējas (jeb pieejamības) laiks 98% mēnesī. No tā izriet, ka, lai sasniegtu e-pakalpojuma darbspēju ne mazāku kā 98% mēnesī, arī ar e-pakalpojuma darbību saistītajām IS un pārējiem tehniskajiem resursiem izvirzītais pieejamības rādītājs nevar būt iestādēs noteikts zemāks kā 98% mēnesī.

Sasniedzamais pieejamības līmenis ir jāsalāgo ne tikai starp konkrēto e-pakalpojumu, to atbalstošo IS, IKT infrastruktūru un integrētajām IS, bet arī attiecībā uz vietu, kur e-pakalpojums ir izmitināts – iestādes mājas lapu vai portālu Latvija.lv, kura darbību un uzturēšanu veic VRAA[14].

Latvija.lv uz 01.05.2022.[15] ir pieejama informācija par 2431 e-pakalpojumiem, no tiem pašā portālā izmitināti 119 e-pakalpojumi, pārējie - iestāžu mājas lapās, uz kuriem portālā Latvija.lv ir publicētas saites.

Pieejamības nodrošināšanā nozīmīga ir arī IKT drošība, ko ievieš IS aizsardzībai. IKT drošības viens no mērķiem ir saglabāt IS pieejamību, novēršot pakalpojumu traucējumus. Līdz ar to IS pieejamība tiek nodrošināta savstarpēji mijiedarbojoties IKT resursu (t.sk. IS) un IKT drošības pārvaldībai (3.attēls).



3.attēls. IKT resursu un IS drošības pārvaldība.

Lai nodrošinātu, ka iestādes darbībai un e-pakalpojumu sniegšanai nepieciešamās IS un citi IKT resursi darbojas un ir pieejami, iestādes nodrošina IS drošības un IKT darbības nepārtrauktības pārvaldību. Tā ir vērsta gan uz incidentu iestāšanās iespējamības un ietekmes minimizēšanu, gan arī uz iestādes spēju incidentus savlaicīgi atklāt un iespējami īsā laikā novērst. Normatīvajos aktos ir noteikti vairāki

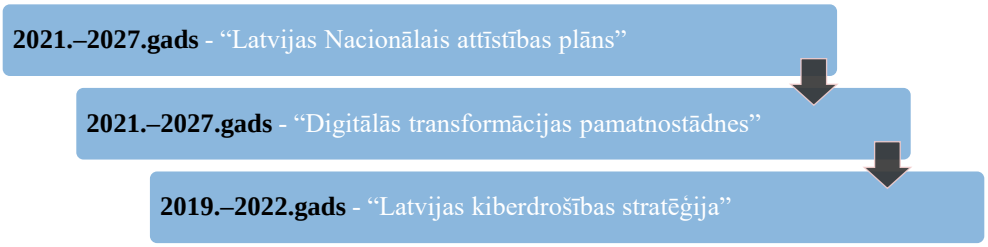
priekšnoteikumi, lai veidotu IS drošības pārvaldībai atbilstošu iekšējās kontroles vidi, kas ir būtiska IS pieejamības nodrošināšanā.

Kontekstā ar IS drošības pārvaldību, kas ir vērsta uz incidentu iestāšanās iespējamības un ietekmes minimizēšanu un uz iestādes spēju incidentus savlaicīgi atklāt, gan IKT darbības nepārtrauktība, gan darbības atjaunošana ir iestādes IS drošības pārvaldības elementi.

Saskaņā ar normatīvajiem aktiem[16] iestādes IKT darbības nepārtrauktības nodrošināšana ir iestādes vadītāja atbildība, apstiprinot drošības politiku un nodrošinot informācijas tehnoloģiju drošības pārvaldību. Normatīvajos aktos ir noteikti vairāki priekšnoteikumi, lai veidotu IS drošības pārvaldībai atbilstošu iekšējās kontroles vidi, kas ir būtiska IS pieejamības nodrošināšanā, tomēr šo priekšnoteikumu ieviešana ir atkarīga no tā, kādu drošības kategoriju iestāde sistēmai ir noteikusi – pamata vai paaugstinātas drošības sistēma[17]. Sasniedzamais IS pieejamības līmenis atkarībā no sistēmai noteiktās drošības kategorijas normatīvajā aktā nav noteikts.

Attiecībā uz IKT infrastruktūras pārvaldību Valsts kontrole revīziju[18] veica 2019. gadā. Tajā konstatēts, ka iestādēs nepietiekama uzmanība tiek pievērsta dažādiem IKT darbības nepārtrauktības jautājumiem, piemēram, netiek pārbaudītas nepārtrauktās elektroenerģijas barošanas iekārtas, nav paralēlo elektrības slēgumu u.c. alternatīvu risinājumu, kas ir būtiski avārijas gadījumā, lai atjaunotu IKT infrastruktūras darbību.

IS pieejamības nozīmīgums ir ietverts vairākos jomas attīstības plānošanas dokumentos (šīs revīzijas kontekstā informatīvais ziņojums[19] kopā ar pamatnostādnēm[20] un plānu[21] ir uzskatāmi par jomas attīstības plānošanas ietvaru un tiks apzīmēti kā "attīstības plānošanas dokumenti"), tādejādi secināms, ka IKT, IS un iestāžu nodrošinātie e-pakalpojumi ir būtisks valsts pārvaldes resurss (4.attēls).



4.attēls. IKT darbības nepārtrauktības un IS pieejamība politikas plānošanas dokumentos.

Raksturojot valstī kopumā noteikto IKT darbības nepārtrauktības, IS un e-pakalpojumu pieejamības nozīmību attīstības plānošanas dokumentos, tajos noteiktie mērķi un uzdevumi vairāk attiecas uz IKT infrastruktūras darbības nepārtrauktības nodrošināšanu, neiezīmējot konkrētus mērķus, uzdevumus un rezultatīvos rādītājus attiecībā uz IS pieejamības līmeni.

Ņemot vērā, ka IS pieejamība tiek nodrošināta savstarpēji mijiedarbojoties IKT resursu (t.sk. IS) un IKT drošības pārvaldībai, tad atbildība par šo funkciju ir sadalīta starp vairākām iestādēm:

- IKT resursu (t.sk. IS un e-pakalpojumu) pārvaldības jomā[22] vadošā iestāde ir VARAM, kas izstrādā politiku, organizē un koordinē politikas īstenošanu. Arī IKT izmantošanā optimālai iestāžu funkciju izpildes organizēšanai un pakalpojumu klāsta un satura pilnveidošanai un pieejamības nodrošināšanai[23].

- IKT drošības jomā vadošā iestāde ir Aizsardzības ministrija, kas koordinē IT drošības politikas veidošanu un īstenošanu[24]. IKT drošības īstenošanā nozīmīga loma ir Informācijas tehnoloģiju drošības incidentu novēršanas institūcijai[25] (turpmāk – CERT.LV), kas uztur vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu, sniedz atbalstu drošības incidentu novēršanā, kā arī uzrauga, kā valsts un pašvaldības iestādes izpilda Informācijas tehnoloģiju drošības likumā noteiktos pienākumus;
- Iestādes līmenī katras iestādes vadītājs nodrošina IKT drošības pārvaldību, t.sk., lemjot par IKT infrastruktūras aizsardzībai piemērojamajiem tehniskajiem līdzekļiem.

Šajā revīzijā Valsts kontroles revidenti gribēja pārliecināties, vai varam paļauties uz IS pieejamību un e-pakalpojumu saņemšanu. Lai uz to atbildētu, šajā revīzijā tika vērtēts:

- Vai valstī vienkopus tiek analizēta informācija par IS un e-pakalpojumu pieejamību un tiek vērtēts, vai e-pakalpojumiem un to atbalstošajām IS normatīvajos aktos noteiktais 98% pieejamības līmenis tiek sasniegts?;
- Vai iestādes ir veikušas nepieciešamās darbības un ir ieviesušas priekšnosacījumus, lai nodrošinātu IS un IKT infrastruktūras darbības nepārtrauktību un atjaunošanu un sasniegtā e-pakalpojumu un IS pieejamības līmeņa mērīšanu?;
- Vai normatīvie akti pietiekami skaidri nosaka priekšnoteikumus, kas iestādēm ir jānodrošina, lai e-pakalpojumi un IS ir pieejamas?;
- Vai politikas plānošanas dokumenti izvirza mērķus un sasniedzamos rezultatīvos rādītājus tik būtiskai iestāžu darbības jomai kā e-pakalpojumu darbība un pieejamība?

Revīzijā tika vērtēta e-pakalpojumu un ar to sniegšanu saistīto tehnisko resursu pārvaldība, pieejamības nodrošināšanai e-pakalpojumu un ar to saistīto IS un IKT infrastruktūras pieejamība. Revīzijā netika vērtēts valsts pārvaldē piedāvāto e-pakalpojumu pilnīgums, saturs un funkcionalitāte (to starp, pieejamība personām ar īpašām vajadzībām).

1. Vai e-pakalpojumu un to atbalstošo IS pieejamība ir sasniegta?

Ko ietekmē e-pakalpojumu un to atbalstošo IS nepieejamība?

Nacionālā līmenī līdz šim nav veiktas aplēses – cik daudz valstij izmaksā IS nepieejamība un kādas sekas uz tautsaimniecību un pakalpojumu saņēmējiem rada IS un e-pakalpojumu nepieejamība. Attiecībā uz valsts pārvaldes iestādēm IS un e-pakalpojumu nepieejamība palielina administratīvo slogu, tiek ietekmēta iestādes reputācija, nespējot nodrošināt pakalpojumu, tiek aizkavēta iestādes darbība kādā jomā vai pakalpojuma izpildes ātrumu, ietekmējot pakalpojuma saņēmēju.

Neviens normatīvais akts neparedz informācijas par e-pakalpojumu un to atbalstošo IS pieejamību apkopošanu. To neparedz normatīvie akti nedz IT drošības jomā, nedz valsts pārvaldes pakalpojumu jomā. Lai gan viens no valsts pārvaldes principiem ir, ka valsts pārvalde savā darbībā pastāvīgi pārbauda un uzlabo sabiedrībai sniegto pakalpojumu kvalitāti, un ir noteikti rādītāji, kas jāmēra un jāpublicē Pakalpojumu sniegšanas un pārvaldības platformā, tomēr tie neietver e-pakalpojuma pieejamības rādītājus.

Revidentu ieskatā kopējās sekas IS un e-pakalpojumu nepieejamībai varētu būt ievērojamas – lai gan CERT.LV pārskatos laikā no 2020. līdz 2021.gadam no [IP] incidentiem, kas saistāmi ar valsts pārvaldi, pašvaldībām un valsts kapitālsabiedrībām, tikai dažos gadījumos ir minēts, ko incidents ir ietekmējis, piemēram, vienā gadījumā vien ietekmēta [IP] valsts un pašvaldību iestāžu vietņu darbība. IS nepieejamības gadījumā sekas rodas ne tikai pašai iestādei, bet arī citām iestādēm, kuras savlaicīgi nesaņem nepieciešamo informāciju, līdz ar to iestādes nevar sniegt pakalpojumus vai arī palēninās to izpildes ātrums.

Revidentu aplēses liecina, ka, ja diennakti nav pieejams portāls Latvija.lv, pakalpojumu saņēmēji nesaņem vismaz 22 500[26] e-pakalpojumus diennaktī. Revīzijā analizējot portālā Latvija.lv publicētos paziņojumus par portāla un e-pakalpojumu darbības traucējumiem četru mēnešu periodā[27], konstatēts, ka kopumā par 21 e-pakalpojumu (jeb 17% no visiem Latvija.lv esošajiem e-pakalpojumiem) ir bijuši paziņojumi, ka e-pakalpojums nedarbojas, no tiem astoņi e-pakalpojumi nedarbojās no vienas līdz 23 dienām, tādējādi secināms, ka tie konkrētajā mēnesī ir bijuši pieejami robežās no 26% līdz 96,8% mēnesī, kas ir mazāk nekā normatīvajā aktā noteiktais

98% sasniedzamais e-pakalpojuma līmenis. 2022.gada pirmā ceturkšņa laikā ar e-pakalpojumu darbības traucējumiem vai to nepieejamību varēja saskarties vismaz 84 000 e-pakalpojumu pieprasītāju (tika novērotas tehniskas problēmas, kā rezultātā e-pakalpojums varēja notikt, bet varēja arī nenotikt). Saskaņā ar aplēsi konkrēto e-pakalpojumu pilnībā varēja nesaņemt 10 000 gadījumos. Arī VRAA uzkrātā informācija par kļūdu skaitu e-pakalpojumu izsaukumos liecina, ka iedzīvotāji bieži sastopas ar e-pakalpojumu izsaukumu kļūdām. Saskaņā ar VRAA uzkrāto informāciju kopumā kļūdu skaits atsevišķiem – nestabilākajiem pakalpojumiem mēdz sasniegt 40–60% (pie ļoti maza servisu izsaukumu skaita, t.i., retāk lietotajiem e-pakalpojumiem – pat 100%). Tādējādi secināms, ka faktiskais e-pakalpojumu saņēmēju skaits, kas sastopas ar e-pakalpojumu darbības traucējumiem vai to nepieejamību, varētu būt pat lielāks nekā revidentu aplēsē aprēķinātais, kas balstīts uz e-pakalpojumu izmantošanas statistiku 2020. gadā.

E-pakalpojuma nepieejamība rada administratīvo slogu gan pakalpojuma saņēmējam, kuram ir jāmeklē alternatīvs risinājums pakalpojuma saņemšanai vai jātērē laiks, pārbaudot, vai pakalpojuma pieejamība ir atjaunota, gan arī valsts pārvaldei, apkalpojot privātpersonu mazāk automatizētā pakalpojumu sniegšanas kanālā. Nenoliedzami, ka faktiskais administratīvais slogs ir atkarīgs no tā, cik būtisku pakalpojumu saņēmējiem IS vai tehnoloģisko platformu nepieejamība ir skārusi un cik ilgi ir bijis pārtraukums. Pēc revīzijā veiktās aplēses secināms, ka e-pakalpojuma nesaņemšana attālinātā veidā kopumā var radīt vismaz 17,23 *euro* administratīvo slogu par katru pakalpojuma nesaņemšanas reizi, no tām pakalpojuma saņēmējam var radīt 15,40 *euro* izmaksas un var nākties patērēt 1,5 stundu laika, lai to saņemtu klātienē, kā arī nelietderīgi tērē iestādes resursus 1,83 *euro* apmērā par vienu pakalpojumu. Tikai viena paša portāla Latvija.lv nepieejamība var radīt administratīvo slogu 16 tūkst. *euro* stundā, jeb 269 *euro* minūtē, savukārt kopumā attiecībā uz revīzijā konstatētajiem 10 tūkst. pakalpojumu nepieejamības gadījumiem varēja tikt radīts administratīvais slogs iedzīvotājiem 162 tūkst. *euro*, savukārt valsts pārvalde – 19,2 tūkst. *euro* varēja izmantot efektīvāk citu funkciju veikšanai.

Lielākā daļa revīzijas izlasē ietverto iestāžu atzīst, ka to rīcībā nav ne datu, ne rīku, ar kuru palīdzību uzraudzīt un mērīt IS un e-pakalpojumu pieejamību. Daļa iestāžu norāda, ka to uzturētās IS ir strādājušas ar augstu pieejamības līmeni, to pamatojot ar to, ka nav novēroti būtiski IKT drošības incidenti, kas būtu ietekmējuši IS pieejamību, tomēr ticamus un viennozīmīgi interpretējamus datus par sasniegto IS pieejamības līmeni šīs iestādes nevar iesniegt – attiecīgi nav nosakāms, vai šo iestāžu IS sasniedz noteikto IS pieejamības līmeni. Tas iezīmē būtisku trūkumu sasniegtā pieejamības līmeņa novērtēšanā – trūkst salīdzināmu uzskaites datu.

IS nepieejamība tautsaimniecībai var izraisīt dažāda veida un apmēra zaudējumus. Zaudējumos, ko izraisa IS nepieejamība, iekļauj zaudēto darījumu izmaksas, zaudētās reputācijas izmaksas, sodu izmaksas, IS darbības atjaunošanas izmaksas un zaudēto darba stundu izmaksas[28].

2020. gadā tika veikts pētījums[29], kas aptvēra 1200 dažāda lieluma uzņēmumus Ziemeļamerikā, Eiropā, Āzijā, Austrālijā, Jaunzēlandē, Dienvidamerikā un Āfrikā. Pētījumā lielākā daļa respondentu (88%) norādījuši, ka viena dīkstāve uzņēmumam ir izmaksājusi ap 300 tūkstošiem dolāru, minot, ka viena dīkstāves stunda IKT nepieejamības dēļ var izmaksāt no 150 tūkstošiem līdz vienam miljonam dolāru.

Attiecībā uz valsts pārvaldes iestādēm IS vai e-pakalpojumu nepieejamība palielina administratīvo slogu[30]. Administratīvais slogs e-pakalpojumu nepieejamības dēļ rodas gan pakalpojumu saņēmējam, gan iestādei, kas nodrošina pakalpojumu sniegšanu, radot gan ar finanšu izdevumiem saistītas izmaksas, gan ar laika patēriņu saistītas izmaksas[31].

Revidentu ieskatā tas ietekmē arī iestādes reputāciju, jo tiek aizkavēta iestādes darbība kādā jomā vai pakalpojuma izpildes ātrums, ietekmējot klientu jeb iedzīvotāju[32].

Latvijā līdz šim nav veiktas aplēses, cik daudz var izmaksāt vai ir izmaksājusi e-pakalpojumu vai IS nepieejamība, un nav dokumentēts, kādas sekas uz tautsaimniecību, iestādi un pakalpojuma saņēmēju IS nepieejamība atstāj.

Statistika par e-pakalpojumu un to atbalstošo IS pieejamību

Revīzijā, vērtējot iespējas un apzinot datus, vai valsts pārvaldē tiek nodrošināta e-pakalpojumu pieejamība normatīvajā aktā[33] noteiktajā līmenī (98% mēnesī), tika konstatēts, ka neviens normatīvais akts neparedz šādas informācijas apkopošanu. To neparedz nedz normatīvie akti IT drošības jomā[34] (detalizēti skatīt ziņojuma 2.sadaļu), nedz valsts pārvaldes pakalpojumu jomā[35].

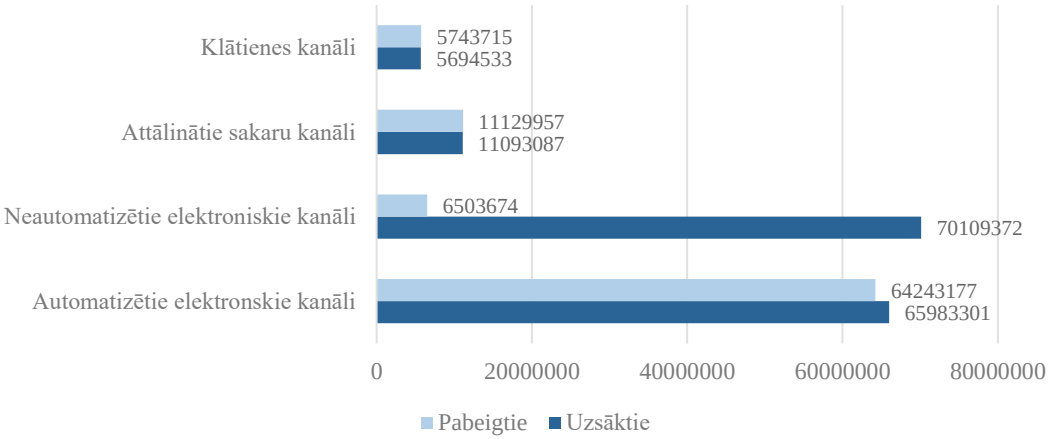
Vērtējot normatīvos aktus attiecībā uz pakalpojumu kvalitāti valsts pārvaldē, konstatēts, ka viens no valsts pārvaldes principiem[36] ir, ka valsts pārvalde savā darbībā pastāvīgi pārbauda un uzlabo sabiedrībai sniegto pakalpojumu kvalitāti. Šim mērķim normatīvais akts nosaka[37]: pakalpojuma sniedzējam Pakalpojumu sniegšanas un pārvaldības platformā ir jāpublicē pakalpojumu izpildes rādītāji:

- pieteikto pakalpojumu gadījumu skaits konkrētam pakalpojumam;
- katram konkrētam pakalpojuma pieteikumam izmantotais kanāls;
- pakalpojumu izpildes kavējumu skaits konkrētam pakalpojumam;
- sūdzību skaits par konkrēto pakalpojumu.

Turklāt, ja iestāde uztur e-pakalpojumus, katram pakalpojumam ir papildus[38] jāmēra:

- e-pakalpojuma izpildes veiksmīgums – pabeigšanas un uzsākšanas gadījumu skaita attiecība;
- pakalpojuma elektroniskas lietošanas pakāpe – elektroniskajā kanālā pieteikto pakalpojumu gadījumu skaita attiecība pret visos kanālos pieteikto pakalpojumu gadījumu skaitu;
- e-pakalpojuma saņēmēja apmierinātība – e-pakalpojuma saņēmēja brīvprātīgs vērtējums piecu punktu sistēmā pēc iespējas par katru e-pakalpojuma sniegšanas gadījumu, kuru var papildināt e-pakalpojuma saņēmēja rakstiska atsauksme.

Revīzijas noslēguma brīdī (2022. gada maijā) pakalpojumu sniegšanas un pārvaldības platformā bija pieejama statistika par iestāžu pakalpojumiem 2020. gadā[39]. Tiek uzkrāta statistika par pakalpojumu uzsākšanu un pabeigšanu 11 dažādos saziņas kanālos (e-pakalpojumi[40], citi elektroniskie, bet neautomatizētie kanāli[41], attālinātie sakari[42] vai klātiene[43]). Kopumā 2020. gadā uzsākti gandrīz 153 miljoni pakalpojumu dažādos sakaru kanālos (no tiem gandrīz 66 miljoni automatizētajos elektroniskajos kanālos), savukārt pabeigti – nepilni 88 miljoni pakalpojumu (no tiem 64 miljoni automatizētajos elektroniskajos kanālos) (5.attēls).



5.attēls. Pakalpojumu uzsākšanas/pabeigšanas statistika dažādos sakaru kanālos 2020.gadā

Jānorāda, ka Pakalpojumu sniegšanas un pārvaldības platformā pieejamie dati nav izmantojami IS un e-pakalpojumu pieejamības novērtēšanā, jo:

- pakalpojums var tikt uzsākts vienā sakaru kanālā, bet pabeigts citā;
- privātpersona var uzsākt e-pakalpojumu un to nepieteikt līdz galam, attiecīgi starpība starp uzsāktajiem un nepabeigtajiem e-pakalpojumiem var būt saistīta gan ar privātpersonas lēmumu e-pakalpojumu nesaņemt, gan arī ar tehniskām problēmām pakalpojumu pabeigt.

VRAA pieejamā informācija par sasniegto e-pakalpojumu pieejamību

Valsts pārvaldē izstrādātie un ieviestie e-pakalpojumi vai saites uz tiem ir pieejami valsts pārvaldes pakalpojumu portālā Latvija.lv. Tajā ir pieejama informācija par 2431 e-pakalpojumu, no tā portālā Latvija.lv ir izmitināti 119 valsts pārvaldes e-pakalpojumi. Pārējie – iestāžu mājas lapās, uz kurām portālā ir norādītas saites.

Lai informētu e-pakalpojuma lietotāju, portālā tiek publicēti paziņojumi par pakalpojumu nepieejamību vai darbības traucējumiem. Vienlaikus VRAA, kas nodrošina pakalpojumu platformas uzturēšanu, nav uzdots uzraudzīt portālā pieejamo iestāžu e-pakalpojumu pieejamību, līdz ar to VRAA neuzkrāj un neanalizē iestāžu e-pakalpojumu pieejamības datus, periodus un nepieejamības iemeslus. VRAA norādīja[44], ka:

- iestādes bieži nenodrošina savu e-pakalpojumu un ar to saistīto resursu pieejamību paredzētajā apjomā, pie kam šī nepieejamība dažkārt ir ilgstoša un nav atbilstošas reakcijas no iestādes puses (e-pakalpojums netiek apturēts, tas vienkārši ilgstoši nestrādā);

- lai gan normatīvie akti[45] paredz pienākumu iestādēm ziņot VRAA un nodrošināt e-pakalpojumu pieejamību, tomēr pēc VRAA aplēsēm 90% gadījumu tieši VRAA, izmantojot automatizēto e-pakalpojumu darbības pieejamības skanēšanu, identificē e-pakalpojumu nepieejamību un informē par to iestādes.

Revīzijā 2021. gada oktobrī un no 2022. gada 1. janvāra līdz 31. martam tika sekots līdzi portālā Latvija.lv publicētajiem paziņojumiem par e-pakalpojumu nepieejamību un tehniskajām problēmām un tika konstatēts, ka:

- kopumā par 21 e-pakalpojumu (jeb 17% no visiem Latvija.lv esošajiem e-pakalpojumiem) ir bijuši paziņojumi, ka e-pakalpojums nedarbojas. No tiem astoņiem e-pakalpojumiem (jeb 6% no visiem Latvija.lv esošajiem e-pakalpojumiem) paziņojums par to, ka e-pakalpojums nedarbojas, bija redzams ilgstoši – no vienas līdz 23 dienām, tādējādi secināms, ka šie e-pakalpojumi konkrētajā mēnesī ir bijuši pieejami robežās no 26% līdz 96,8% mēnesī, kas ir mazāk nekā normatīvajā aktā[46] noteiktais sasniedzamais e-pakalpojuma līmenis, t.i., 98%.

  Piemēram:

  - *2021. gada oktobrī vairāk nekā 14 dienas bija paziņojums, ka nav pieejams PMLP sniegtais e-pakalpojums "Pārbaude, vai persona ir deklarēta norādītajā adresē";*
  - *2022. gada janvārī vairāk nekā četras dienas bija paziņojums, ka nav pieejams Būvniecības valsts kontroles biroja sniegtais e-pakalpojums "Aizsargātā lietotāja statusa noteikšana";*
  - *2022. gada janvārī septiņas dienas bija paziņojums, ka nav pieejams VSAA sniegtais e-pakalpojums "Informācija par piešķirtajiem VSAA pakalpojumiem", savukārt martā 23 dienas bija paziņojums, ka nav pieejams e-pakalpojums "Informācija par veiktajiem VSAA maksājumiem un no tiem ieturēto ienākuma nodokli (ienākumu deklarēšanai)".*

- Portālā vairākkārt bija publicēti paziņojumi par iespējamajiem traucējumiem e-pakalpojumu darbībā:

  - vidēji 4% no portāla darbības laika bija publicēti paziņojumi par to, ka "tehnisku iemeslu dēļ" iespējami traucējumi e-pakalpojumu un portāla darbībā. *Piemēram, 2022. gada janvārī bija paziņojumi ar kopējo ilgumu vairāk nekā 83 stundas (jeb 11% no portāla darba laika janvārī) par to, ka "tehnisku iemeslu dēļ" iespējami e-pakalpojumu un portāla darbības traucējumi;*
  - vidēji 12% no portāla darbības laika bija publicēti paziņojumi par "iespējamiem traucējumiem saistībā ar autentifikāciju portālā". Piemēram: *2022. gada janvārī un februārī kopā 216 stundas nebija pieejama juridisko personu autentifikācija dēļ tehniskajiem darbiem Uzņēmumu reģistrā.*

Revīzijas izlasē ietvertajās iestādēs pieejamā informācija par sasniegto e-pakalpojumu un to atbalstošo IS pieejamību

Revīzijā, vērtējot revīzijas apjomā iekļautajās deviņās iestādēs sasniegto e-pakalpojumu un to atbalstošo IS pieejamību:

- trīs iestādes informēja, ka, lai gan dažos mēnešos pieejamība kādai IS vai e-pakalpojumam ir pazeminājusies zem 98%, tomēr gada griezumā visām IS un e-pakalpojumiem tiek pārsniegta 98% pieejamība;
- sešas iestādes vai nu nesniedza datus, vai nu norādīja, ka to rīcībā nav datu par IS pieejamības rādītājiem. Iestādes skaidro, ka to rīcībā nav tāda rīka (automatizēta uzraudzības risinājuma) un nav izvirzītu uzraugāmo kritēriju, ar kuru palīdzību uzkrāt datus un noteikt IS pieejamību. Iestādes veic IKT resursu kritisko robežu uzraudzību (piemēram, datu bāzes "*up-time*" rādītājs), kas ir tikai daļa no tehniskajiem resursiem, kuri ir iesaistīti IS darbībā un e-pakalpojuma nodrošināšanā.

  Kopumā iestādes uzskata, ka sasniedz noteiktos pieejamības radītājus, pamatojot to ar faktu, ka gada laikā nav konstatēti būtiski IS drošības incidenti.

CERT.LV apkopotā informācija par IT drošības incidentiem un tās izmantošana sasniegtās pieejamības noteikšanai

CERT.LV uztur vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu[47]. Reizi ceturksnī CERT.LV sagatavo pārskatu par uzdevumu izpildi[48] AiM, kurā tiek ietverta informācija arī par IT drošības incidentiem valsts pārvaldē. Šie pārskati tiek publicēti CERT.LV tīmekļvietnē, tajos atstājot vispārpieejamu informāciju, kas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju.

Izvērtējot pārskatus par 2020. un 2021. gadu, revidenti konstatējuši [IP] ar valsts pārvaldi saistītu incidentu. Ņemot vērā, ka CERT.LV rīcībā nav informācijas, kā savā starpā saslēgtas iestāžu IS un kāda ir to savstarpējā atkarība, tad tikai atsevišķos gadījumos ir minēts, ko incidents ir ietekmējis, un tikai attiecībā uz tehnisko resursu apjomu, nevērtējot ietekmēto privātpersonu vai iestāžu loku. Piemēram:

- *2021. gada 10. oktobrī traucēta Valsts kancelejas uzturētās Valsts un pašvaldību iestāžu tīmekļvietņu vienotās platformas darbība. Tehniska kļūme uz laiku apturēja* [IP] *platformā izvietoto tīmekļa vietņu darbību;*
- [IP]

Jānorāda, ka CERT.LV pārskatos nav pieejama arī cita būtiska informācija – incidenta un attiecīgi IS un e-pakalpojumu nepieejamības ilgums. Tas ir būtiski, lai aplēstu un izdarītu secinājumu par privātpersonām un valsts pārvaldes iestādēm, kuras šī nepieejamība ir ietekmējusi.

IS un e-pakalpojumu nepieejamības sekas

Īpaši pandēmijas apstākļos, kad iestāžu darbība un to sniegtie pakalpojumi lielākoties tika nodrošināti tikai attālinātā veidā, pakalpojumu saņēmēji vistiešāk varēja izjust IS un e-pakalpojumu nepieejamības sekas, jo nevarēja saņemt iestādes pakalpojumus. Piemēram, 2021.gada 5.februārī iedzīvotāju lielās aktivitātes dēļ, piesakoties uz Covid-19 vakcīnas saņemšanu, uz vienu diennakti tika paralizēta portāla Latvija.lv darbība un šajā dienā nebija pieejami vismaz 125 portālā Latvija.lv izmitinātie e-pakalpojumi. Ņemot vērā, ka portāls Latvija.lv faktiski nebija pieejams uz vienu diennakti, pakalpojumu saņēmējiem, kas vēlējās izmantot portālu Latvija.lv pakalpojumu saņemšanai, tika liegts saņemt vismaz 22 500[49] e-pakalpojumus.

Turklāt, ņemot vērā, ka portāls Latvija.lv nebija pieejams diennakts garumā, neviens portālā Latvija.lv izmitinātais e-pakalpojums mēneša griezumā vairs nevarēja sasniegt normatīvajā aktā[50] noteikto sasniedzamo pieejamības līmenī 98%.

Ņemot vērā, ka valsts pārvaldē nav vērtēta e-pakalpojumu un IS nepieejamības ietekme tāpat kā vienkopus nav apzināta un analizēta arī IS un e-pakalpojumu pieejamība, revidenti no 2022. gada 1. janvāra līdz 31. martam analizēja portālā Latvija.lv publicētos paziņojumus par e-pakalpojumu darbības traucējumiem vai nepieejamību.

Kopumā katru dienu bija publicēti paziņojumi, kas saistīti ar portāla Latvija.lv vai ar tā izmantošanu saistīto moduļu darbību vai konkrētu e-pakalpojumu pieejamību (skatīt 5.tabulu).

Saskaņā ar paziņojumiem par traucējumiem portāla darbībā, kas ietekmēja tālāku piekļuvi arī e-pakalpojumiem, portāla Latvija.lv pieejamība tika traucēta vai netika nodrošināta 905 stundas. Vidēji dienā portālā tiek veikti 22,5 tūkst. pieprasījumi, līdz ar to kopumā 84 tūkst. gadījumos tika ietekmēta portāla izmantošana.

Tāpat konstatēts, ka kādu brīdi (kopsummā 1093 stundas) nebija pieejami 20 e-pakalpojumi, kas vidēji tiek izmantoti 6870 reizes dienā, līdz ar to par visu nepieejamības periodu netika nodrošināti 10 tūkst. e-pakalpojumu pieprasījumi.

1.tabula

Aplēse par portāla Latvija.lv darbības traucējumiem vai to nepieejamību 2022.gada 1.ceturksnī

Traucējuma būtība	Paziņojuma ilgums (stundās)	Nepieejamība % no portāla darbības laika[51]	Izmantošanas reižu skaits 2021.gada 1.ceturksnī[52] (pieprasījumu skaits)	Traucējumu dēļ ietekmēto pieprasījumu skaits
Iespējami traucējumi portāla un e-pakalpojumu darbībā tehnisku iemeslu vai tehnisku darbu dēļ[53]	90,51	**4%**	2 055 622	83 949
Iespējami traucējumi vai nestrādās autentifikācija portālā[54]	243	**12%**	-	-
Traucējumi maksājumu veikšanā[55]	26,26	**1,1%**	-	-
Traucējumi e-adreses darbībā[56]	2640	**100%**	-	-

Traucējuma būtība	Paziņojuma ilgums (stundās)	Nepieejamība % no portāla darbības laika[51]	Izmantošanas reižu skaits 2021.gada 1.ceturksnī[52] (pieprasījumu skaits)	Traucējumu dēļ ietekmēto pieprasījumu skaits
Tehnisku iemeslu dēļ uz laiku var būt apgrūtināta lauku aizpildīšana VSAA e-iesniegumos	840	**40%**	696 075	278 430
E-pakalpojums un traucējuma būtība	**Paziņojuma ilgums (stundās)**	**Nepieejamība % no portāla darbības laika[57]**	**Uzsākšanas reižu skaits 2021.gada 1.ceturksnī[58]**	**Traucējumu dēļ ietekmēto pieprasījumu skaits paziņojuma ilguma periodā**
4 VZD e-pakalpojumi[59]	16	**0,18% (katram pakalpojumam)**	15 603	28
"Aizsargātā lietotāja statusa noteikšana" (BVKB)	110,16	**4,93%**	2808	139
"Mani dati Fizisko personu reģistrā" (PMLP)	24	**1,10%**	49 026	528
"Dzīvesvietas deklarēšana vai norādīšana" (PMLP)	48	**2,15%**	81 535[60]	1754
9 VSAA e-pakalpojumi[61]	4,5	**0,03% (katram pakalpojumam)**	212 819	53
"Informācija par veiktajiem VSAA maksājumiem un no tiem ieturēto ienākuma nodokli" (VSAA)	552,5	**24,76%**	4505	1116
"Pensiju 2.līmeņa dalībnieka konta izraksts" (VSAA)	72,5	**3,25%**	126 362	4108
"Informācija par piešķirtajiem VSAA pakalpojumiem" (VSAA)	168,5	**7,55%**	37 204	2810
"E-iesniegums ģimenes valsts pabalsta un piemaksas pie ģimenes valsts pabalsta par bērnu ar invaliditāti piešķiršanai" (VSAA)	96,5	**4,37%**	-	-

E-pakalpojuma nepieejamība rada administratīvo slogu gan pakalpojuma saņēmējam, kuram ir jāmeklē alternatīvs risinājums pakalpojuma saņemšanai vai jātērē laiks, pārbaudot, vai pakalpojuma pieejamība ir atjaunota, gan arī valsts pārvaldei, apkalpojot pakalpojuma saņēmēju mazāk automatizētā pakalpojumu sniegšanas kanālā.

Saskaņā ar revīzijā veikto aplēsi (2.tabula) e-pakalpojuma nesaņemšana attālināta veidā var radīt vismaz 17,23 *euro* administratīvo slogu par katru pakalpojuma nesaņemšanas reizi, no tām pakalpojuma saņēmējam var radīt 15,40 *euro* izmaksas un pakalpojuma saņēmējam var nākties patērēt 1,5 stundu laika, lai to saņemtu klātienē, kā arī nelietderīgi var tikt tērēti iestādes resursi - 1,83 *euro* apmērā par vienu pakalpojumu. Kopumā attiecībā uz revīzijā konstatētajiem 10 tūkst. pakalpojumu nepieejamības gadījumiem varēja tikt radīts administratīvais slogs pakalpojumu saņēmējiem 162 tūkst. *euro*, kā arī valsts pārvalde pakalpojuma sniegšanai ne-elektroniskā veidā 19,2 tūkst. *euro* varēja izmantot efektīvāk citu funkciju veikšanai.

2.tabula

Aplēse – ietekme, kas rodas e-pakalpojumu nepieejamības dēļ

	Viens pakalpojums	2022. gada janvāris–marts	
		Viena darba diena	Kopā
E-pakalpojumu pieprasījumi, kas netika nodrošināti		165 reizes	10532 reizes
Ietekme uz iestāžu darbu			
Pakalpojuma apkalpošana klātienē	15 min[62]	41 stunda	2633 stundas
Iestādes darbinieka patērētā laika izmaksas	1,83 *euro* (15 min. no vidējās algas likmes valsts pārvaldē[63] pirms nodokļu nomaksas)	165 *euro*	19223 *euro*
Ietekme uz iedzīvotāju			
Iedzīvotāja laika patēriņš iestādes apmeklējumam klātienē	1,5 stundas[64]	247 stundas	15798 stundas
Iedzīvotāja patērētā laika izmaksas	13,08 *euro* (1,5 stunda no vidējās algas likmes[65] pirms nodokļu nomaksas)	2152 *euro*	137 759 *euro*
Sabiedriskā transporta izmaksas	2,30 *euro*[66]	378 *euro*	24224 *euro*
Izmaksas iedzīvotājam (kopā):	**15,40 euro**	**2531 euro**	**161982 euro**

Nenoliedzami, ka faktiskais administratīvā sloga apmērs ir atkarīgs no tā, cik būtisku e-pakalpojumu nepieejamība ir skārusi un cik ilgs ir bijis pārtraukums. Piemēram, portāla Latvija.lv darbības pārtraukums uz vienu diennakti pēc revidenta aplēses var radīt administratīvo slogu 388 tūkst. *euro* diennaktī[67] jeb 16 tūkst. *euro* stundā.

Ieteikums

Lai valstiski identificētu jomas, kurās e-pakalpojumu un to atbalstošo IS un IKT resursu pieejamība ir būtiski stiprināma, VARAM:

- *nodrošināt, ka valsts pārvaldes IKT infrastruktūras koplietošanas pakalpojumu sniedzēju sniegtajiem pakalpojumiem tiek nodrošināta pakalpojumu pieejamības uzskaite, kas ietver gan infrastruktūras, gan arī tās atbalstīto lietojumu (sistēmu) pieejamības monitoringu un vienveidīgu uzskaiti;*
- *regulāri nodrošināt konsolidēta pārskata sagatavošanu par sasniegto pieejamības līmeni visiem valsts pakalpojumus nodrošinošiem IKT resursiem, to starp, vērtējot kādas sekas valstij un iedzīvotājam atstāj, ja pieejamība netiek sasniegta.*

Vai e-pakalpojumu un to atbalstošo IS pieejamību ietekmē IT drošības incidents?

Lai gan iestāžu incidentu reģistros uzkrāto datu analīze varētu sekmēt iestādēs sasniegtā IS un e-pakalpojumu pieejamības līmeņa novērtēšanu, tomēr iestāžu incidentu reģistru dati ir nepilnīgi – sešas no deviņām revīzijas apjomā iekļautajām iestādēm ir norādījušas, ka neuzrauga e-pakalpojumu pieejamību, līdz ar to var būt gadījumi, kad pārtraukumi e-pakalpojuma darbībā netiek fiksēti un reģistrēti, savukārt tikai trīs iestādēs ir ieviesta prakse, ka incidentu reģistrā vai kādā citā atsevišķā reģistrā tiek uzkrāta informācija par visiem plānotajiem tehnisko darbu datumiem un pārtraukumu ilgumiem. Jānorāda, ka revīzijas laikā divas iestādes neiesniedza incidentu reģistra datus, tādējādi liedzot novērtēt, vai šo iestāžu incidentu reģistros tiek uzkrāta informācija par incidentiem, kas būtu varējuši ietekmēt iestāžu IS darbības nepārtrauktību un sasniedzamo IS pieejamības līmeni.

Nacionālā līmenī informāciju par iestādēs notikušajiem IT drošības incidentiem uzkrāj CERT.LV, tomēr ne par visiem notikušajiem incidentiem CERT.LV ir informēta, jo iestādēs nav vienotas pieejas, kad informācija CERT.LV ir jāsniedz.

Arī no CERT.LV pārskatos uzrādītās informācijas revidenti nevarēja gūt visaptverošu priekšstatu par faktisko IT drošības incidentu skaitu un ietekmētajām iestādēm, jo informācija pārskatos tiek atspoguļota atšķirīgā griezumā - pārskatos tiek iekļauta informācija par ietekmētajām IP adresēm, un tikai atsevišķos gadījumos tiek apskatīta situācija (IT drošības incidenti) konkrētās iestādēs. Aizsardzības ministrijai iesniegtajos ierobežotas pieejamības pārskatos [IP] incidentu valsts pārvaldes iestādēs, pašvaldībās vai valsts kapitālsabiedrībās ir saistīti ar pakalpojuma pieejamības traucējumiem. Turklāt CERT.LV rīcībā nav informācijas par IT drošības incidentā ietekmētajām IS, ja iestādes tās nav pieminējušas IT drošības incidenta aprakstā.

Valstiskā līmenī netiek uzkrāta informācija par cēloņiem, kas ietekmējuši IS pieejamību, bet pēc revidentu veiktās aptaujas rezultātiem secināms, ka neplānoto nepieejamību 34% gadījumu izraisīja pašas IS darbības problēmas vai IKT incidenti, 28% gadījumu – elektrības pārrāvumi, 25% gadījumu – tehnisko resursu darbības problēmas.

Revidentu ieskatā, valstiskā līmenī analizējot datus ne tikai par valstī notiekošajiem IT drošības incidentiem, bet arī par visiem IS nepieejamības gadījumiem vai darbības traucējumiem, jau valstiskā mērogā varētu nodrošināt preventīvu rīcību, kas būtu vērsta uz iepriekš bijušu incidentu un cēloņu, kas ietekmē IKT darbības nepārtrauktību un IS pieejamību, rašanās iespējamības samazināšanu vai pat novēršanu nākotnē.

CERT.LV ir izveidojusi sensoru tīklu, kas nodrošina datu plūsmas anomāliju analīzi, ļaunatūras atpazīšanu un brīdinājumu saņemšanu par konstatētajiem apdraudējumiem iestādes datortīklā, [IP].

Iestādēs uzkrātā informācija par IT drošības incidentiem

IS un e-pakalpojumu pieejamību ietekmē gan plānotie pārtraukumi IS darbībā (darbi IS atjaunošanai un konfigurācijai), gan neplānoti pārtraukumi IS darbībā (pārtraukumi, kuri radušies dažādu incidentu gadījumos), gan IS vai e-pakalpojuma funkcionāli traucējumi.

Neplānoti pārtraukumi IS darbībā var rasties arī no iestādes neatkarīgu iemeslu dēļ. Piemēram, datu pārraides tīkla pārrāvumu dēļ ir pārtraukta IS pieejamība no ārpuses, savukārt iestādes iekšienē IS būs pieejama un darbosies

Revīzijā izlasē ietvertajās iestādēs konstatēts, ka iestāžu iekšējie normatīvie akti paredz un apraksta incidentu reģistrēšanas un analīzes procedūras, kā arī paredz incidentu reģistrēšanu atsevišķos reģistros. Saskaņā ar iestāžu sniegto informāciju (jānorāda, ka divas iestādes neiesniedza incidentu reģistra datus, tādējādi liedzot tos novērtēt) par incidentu reģistros uzkrāto informāciju par incidentiem laikā no 2019. gada janvāra līdz 2021. gada septembrim:

- četrās iestādēs ir fiksēti incidenti, kas ietekmējuši IS pieejamību, savukārt trīs iestādes ir norādījušas, ka šajā laikā to uzturētajām IS nav novēroti tādi incidenti, kas ietekmētu to pieejamību – attiecīgi arī incidentu reģistros nav pieejami ar IS pieejamību saistīti ieraksti. Tai pašā laikā incidentu reģistros iestādes uzkrāj lietotāju pieteiktās problēmas attiecībā uz to, ka nav pieejams kāds informācijas resurss, kas pēc iestāžu domām nav traucējis IS darbībai;
- vienā iestādē konstatēts, ka 2021. gadā CERT.LV ir fiksējis incidentu saistībā ar iestādes uzturētās valsts IS TLS sertifikātu, kas radīja IS pieejamības problēmas lietotājiem, tomēr pati iestāde Valsts kontrolei norādīja, ka šajā laika periodā tās incidentu reģistrā nav nonācis neviens pieteikums par IS nepieejamību;
- tikai trīs iestādēs ir ieviesta prakse, ka incidentu reģistrā vai kādā citā atsevišķā reģistrā tiek uzkrāta informācija par visiem plānotajiem tehnisko darbu datumiem un pārtraukumu ilgumiem;
- attiecībā uz e-pakalpojumiem sešas no revīzijas apjomā iekļautajām iestādēm, kuru IS nodrošina e-pakalpojumu sniegšanu, ir norādījušas, ka neuzrauga e-pakalpojumu pieejamību, līdz ar to var būt gadījumi, kad ar e-pakalpojumu saistītā IS darbojas, bet pats e-pakalpojums nav pieejams, bet e-pakalpojuma pārtraukums incidentu reģistrā netiek fiksēts un reģistrēts.

Kā labā prakse minama, ka saistībā ar incidentu izvērtēšanu vienā iestādē tiek praktizēts par incidentiem sastādīt ziņojumus un ziņojumos paredzēt preventīvās darbības nākotnē, lai incidents neatkārtotos, savukārt pārējās iestādēs ir noteiktas procedūras IKT incidentu izvērtēšanai un informācija par IKT incidentiem pēc iespējas tiek iekļauta ikgadējā iestādes IKT risku analīzē.

Nacionālā līmenī uzkrātā informācija par IT drošības incidentiem

No likuma izriet[68], ka valsts vai pašvaldības institūcija drošības incidenta gadījumā nekavējoties veic visas tā novēršanai nepieciešamās darbības, kā arī tūlīt informē par notikušo CERT.LV.

Informācijas tehnoloģiju drošības incidents[69] ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

CERT.LV savā mājas lapā līdz 16.02.2021. norādīja[70]:

> *Valsts un pašvaldības iestādes IT drošības pārzinim jāziņo par incidentu, ja ir noticis ārējs vai iekšējs uzbrukums iestādes IT infrastruktūrai un šī uzbrukuma rezultātā notikusi svarīgu resursu atteice, kā arī apgrūtināta iestādes normāla darbība vai būtisku pakalpojumu sniegšana.*
>
> *Likums paredz informēt CERT.LV tikai par incidentiem un būtiskām sistēmiskām vājībām, kas var apdraudēt informācijas tehnoloģiju integritāti, pieejamību un konfidencialitāti, piemēram, ievainojamībām valsts informācijas sistēmu produkcijas vidēs, ievainojamībām, kas var ietekmēt saistītās ārējās informācijas sistēmas, iestādes pamatfunkciju nodrošināšanu u.c.*
>
> *Reizē norādām, ka likums neparedz izņēmumu attiecībā uz „iekšējo" informācijas sistēmu incidentiem un drošības nepilnībām.*

Revīzijā konstatēts, ka iestādēs nav vienotas pieejas par gadījumiem, kad informēt CERT.LV – vai informēt tikai par tādiem IT drošības notikumiem, kas ir pēkšņi, negaidīti un neizskaidrojami, vai arī par tādiem, kas radušies neveiksmīgu, bet plānotu tehnisku uzlabojumu rezultātā. Piemēram, nekorekti konfigurējot IS vai neveiksmīgas IKT infrastruktūras nomaiņas rezultātā zaudēta tās pieejamība. Papildus – iestādēm nav noteikta ziņošanas forma, kādā tām jāziņo CERT.LV par IT drošības incidentu. Saskaņā ar CERT.LV mājas lapā norādīto informāciju informācija par IT drošības incidentu ir jānosūta brīvā formā uz CERT.LV e-pastu[71].

Attiecībā uz pamatpakalpojumu un digitālā pakalpojuma sniedzējiem ir noteikta detalizētāka metodika[72], kas paredz pakalpojuma sniedzējam vērtēt incidenta būtiskumu, ņemot vērā skarto lietotāju skaitu un dīkstāves ilgumu, un ziņošanas forma (6.attēls).

***Būtiskas ietekmes uz pakalpojuma nepārtrauktību novērtēšana**

	Dīkstāve				
Skartie lietotāji	**0 h**	**1-2 h**	**2-4 h**	**4-24 h**	**> 24 h**
0					•
1-10% (ieskaitot)				•	•
10-15% (ieskaitot)			•	•	•
≥ 1 lietotājs citā ES valstī			•	•	•
≥ 15%		•	•	•	•
≥ 1 lietotājs, kurš ir lielo uzņēmumu sarakstā	•	•	•	•	•
≥ 1/4 no lietotājiem kādā no Latvijas plānošanas reģioniem	•	•	•	•	•

6.attēls. Metodika IT drošības incidenta būtiskuma identifikācijai un ziņošanai CERT.LV

CERT.LV analizē IT drošības incidentus, tostarp tādus, kuri ir izraisījuši IS darbības traucējumus, tomēr valstiskā līmenī šī informācija netiek tālāk analizēta.

Revidentu ieskatā, valstiskā līmenī analizējot datus ne tikai par valstī notiekošajiem IKT incidentiem, bet arī par visiem IS nepieejamības gadījumiem vai darbības traucējumiem, jau valstiskā mērogā varētu nodrošināt preventīvu rīcību, kas būtu vērsta uz iepriekš bijušu incidentu un cēloņu, kas ietekmē IKT darbības nepārtrauktību un IS pieejamību, rašanās iespējamības samazināšanu vai pat novēršanu nākotnē.

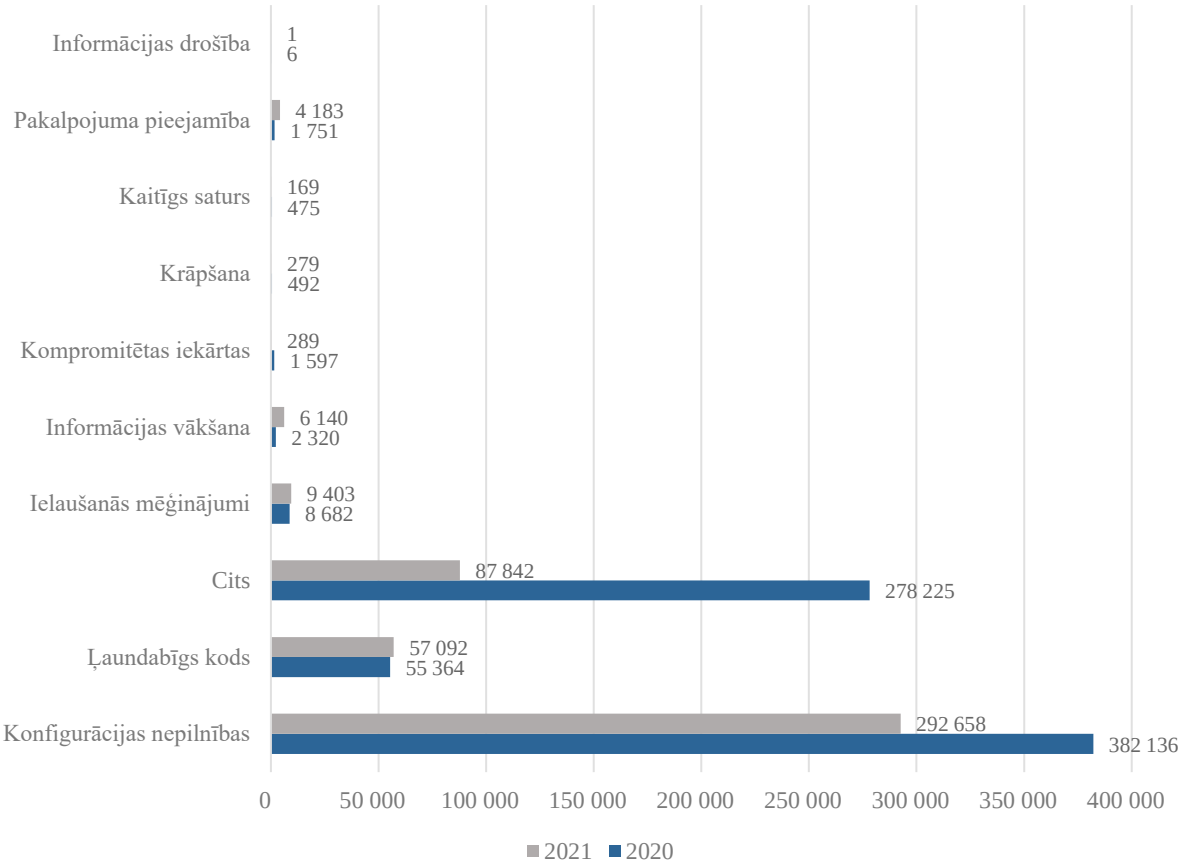
Bez tā, ka iestādēm ir jāziņo CERT.LV par notikušajiem incidentiem, CERT.LV ir izveidojusi[73] sensoru tīklu, kas nodrošina datu plūsmas anomāliju analīzi, ļaunatūras atpazīšanu un brīdinājumu saņemšanu par konstatētajiem apdraudējumiem iestādes datortīklā.

[IP]

[IP]

Vērtējot CERT.LV uzkrātos datus par IT drošības incidentiem, konstatēts, ka netiek uzkrāta pilnīga informācija par IT drošības incidenta ietekmi un to, kādas IS IT drošības incidents ir ietekmējis, jo CERT.LV rīcībā nav informācijas par IT drošības incidentā ietekmētajām IS, ja iestādes tās nav pieminējušas IT drošības incidenta aprakstā. Līdz ar to CERT.LV apzina un statistikas pārskatos iekļauj IT drošības incidenta ietekmēto IP adrešu skaitu, bet tas neļauj iegūt priekšstatu par ietekmētajiem e-pakalpojumiem vai IS un vērtēt rādītājus, kas saistīti ar IS vai e-pakalpojumu pieejamību. CERT.LV skaidroja, ka uzturēt informāciju par IS savstarpējo integrāciju nebūtu racionāli, jo informācija ir apjomīga un to ir nepieciešams uzturēt aktuālu, līdz ar to CERT.LV strādā ar to informācijas apjomu, ko iestāde ir norādījusi.

Atbilstoši CERT.LV pārskatiem 2020. un 2021.gadā Latvijā kopumā IT drošības incidentu dēļ bija ietekmētas gandrīz 1,2 milj. unikālās IP adreses (7.attēls). Uz lielāko daļu IP adrešu (57% no visām ietekmētajām IP adresēm divu gadu periodā) ietekmi ir atstājuši IT drošības incidenti, kas saistīti ar IS vai IKT infrastruktūras konfigurācijas nepilnībām. No publiskajiem pārskatiem secināms, ka 2021.gadā divkārt pieaudzis IP adrešu skaits, kas saistīts ar IS pieejamības traucējumiem, kas radušies piekļuves lieguma uzbrukumu dēļ, kā arī atsevišķu lokālu darbību, piemēram, elektroenerģijas padeves traucējumu vai cilvēciskas kļūdas dēļ (no 1751 IP adreses 2020.gadā līdz 4183 IP adresēm 2021.gadā).



7.attēls. CERT.LV statistika par drošības incidentos ietekmētajām IP adresēm 2020. un 2021. gadā

Tāpat revīzijā konstatēts, ka CERT.LV sagatavotie publiskie pārskati nesniedz pietiekamu priekšstatu par situāciju iestādēs – IT drošības incidentu skaitu, incidenta veidu un ietekmi.

Lai gan CERT.LV pārskatos tiek iekļauta informācija par CERT.LV fiksētajos IT drošības incidentos ietekmētajām IP adresēm un vispārīgiem aprakstiem par incidentu būtību un apdraudējuma veidiem, tomēr tikai atsevišķos gadījumos tiek detalizēti aprakstīti konkrēti IT drošības incidenti iestādēs – attiecīgi, analizējot tikai CERT.LV pārskatos uzrādīto informāciju, revidenti nevarēja gūt visaptverošu priekšstatu par faktisko IT drošības incidentu skaitu un ietekmētajām iestādēm.

Piemēram, laikā no 2020.gada līdz 2021.gadam CERT.LV incidentu reģistrā ir uzkrāta informācija par [IP] IT drošības incidentiem valsts pārvaldes iestādēs, pašvaldībās un valsts kapitālsabiedrībās, savukārt CERT.LV sagatavotajos ierobežotas pieejamības pārskatos, kas tiek sniegti Aizsardzības ministrijai, identificējami [IP] IT drošības incidenti, kas saistāmi ar valsts pārvaldes iestādēm, pašvaldībām un valsts kapitālsabiedrībām. No tiem tikai 141 IT drošības incidents ir atrodams CERT.LV sagatavotajos publiskajos pārskatos, kas tiek publicēti CERT.LV mājas lapā (3.tabula).

Lai gan primāri katrai iestādei ir jāanalizē IT drošības incidenta ietekme, arī CERT.LV tiek uzkrāta informācija, kas ir nozīmīga, lai ne tikai katra iestāde var vērtēt savus iekšējos IKT pārvaldības procesus un to efektivitāti, bet arī attīstības plānošanas dokumentu un normatīvo aktu līmenī plānotu nepieciešamās izmaiņas.

3.tabula

CERT.LV uzkrātā un publicētā informācija par IT drošības incidentiem valsts pārvaldes iestādēs, pašvaldībās un valsts kapitālsabiedrībās laikā no 2020. līdz 2021.gadam

Gads	Incidentu skaits		
	CERT.LV incidentu reģistrs	CERT.LV pārskati Aizsardzības ministrijai (norādot konkrētas iestādes)	CERT.LV publiskie pārskati (nenorādot konkrētas iestādes)
2020	[IP]	[IP]	67
2021	[IP]	[IP]	74
Kopā:	[IP]	[IP]	**141**

Saskaņā ar CERT.LV sniegto informāciju no [IP] IT drošības incidentiem valsts pārvaldes iestādēs, pašvaldībās un valsts kapitālsabiedrībās laikā no 2020. gada līdz 2021. gadam [IP] IT drošības incidenti ir bijuši piecās revīzijas apjomā iekļautajās iestādēs (4.tabula).

4.tabula

Revīzijas apjomā iekļauto iestāžu incidenti CERT.LV reģistrā laikā no 2020. gada līdz 2021. gadam

[IP]

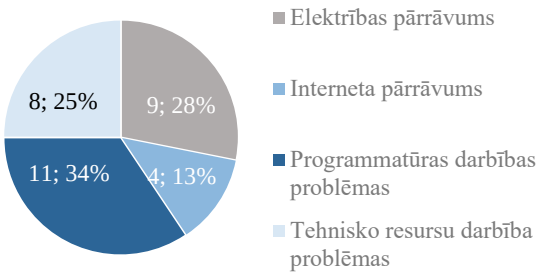
Saskaņā ar CERT.LV sagatavotajiem ierobežotas pieejamības pārskatiem no [IP] incidentiem, kas saistāmi ar valsts pārvaldi, pašvaldībām un valsts kapitālsabiedrībām un par kuriem sniegta informācija CERT.LV laikā no 2020.gada līdz 2021.gadam (8.attēls), lielākā daļa incidentu cēloņu ([IP] jeb 22%) ir saistāmi ar ielaušanās mēģinājumiem nesankcionēti piekļūt sistēmām vai servisiem. Savukārt otrs lielākais incidentu skaits ([IP] jeb 15%) ir saistāms ar dažādu ievainojamību atklāšanu iestāžu IS vai programmatūrās.

[IP]

8.attēls. Incidentu skaits valsts pārvaldes iestādēs, pašvaldībās un valsts kapitālsabiedrībās laikā no 2020.gada līdz 2021.gadam pēc CERT.LV datiem, kas sniegti Aizsardzības ministrijai.

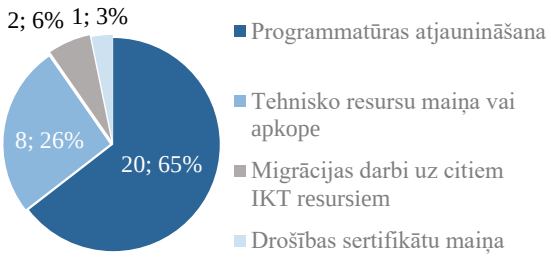
Ņemot vērā, ka valstiskā līmenī netiek uzkrāta informācija par cēloņiem, kas ietekmējuši IS pieejamību, revidentu aptaujā par nacionālā līmeņa IS, kas apmainās ar datiem ar citu valstu IS, tika iekļauti jautājumi par iemesliem, kuri ir izraisījuši IS nepieejamību:

- neplānotās dīkstāves iemesli (9.attēls) ir saistīti ar iestādes IS programmatūras darbības problēmām, elektrības pārrāvumiem, tehnisko resursu darbības problēmām vai interneta darbības pārtraukumiem;



9.attēls. Galvenie neplānotās nepieejamības iemesli

- plānota dīkstāve lielākā daļā gadījumu ir saistīta (10.attēls) ar iestādes nodrošinātu programmatūras atjaunināšanu, kas ir neatņemama IS uzturēšanas sastāvdaļa. Tāpat arī ar tehnisko resursu maiņu vai apkopi, migrāciju uz citiem IKT resursiem vai drošības sertifikātu maiņu.



Ieteikumi

Lai pilnveidotu pieeju, kad un kā iestādēm ir jāinformē CERT.LV par IT drošības incidentiem, ierosinām Aizsardzības ministrijai (kā vadošajai iestādei, kas koordinē IT drošības politikas veidošanu un īstenošanu) sadarbībā ar CERT.LV izstrādāt vadlīnijas, pēc kurām iestādes nosaka IT drošības incidenta būtiskumu un to, vai ir nepieciešams informēt CERT.LV, kā arī noteikt ieteicamo iesniedzamo informācijas apjomu un struktūru.

Lai operatīvi atklātu informāciju par ietekmētajām IS un e-pakalpojumiem un ilgtermiņā sniegtu informāciju par dīkstāves laiku, aicinām Aizsardzības ministrijai sadarbībā ar VARAM izstrādāt datu apmaiņas mehānismu un vienotu informācijas uzkrāšanas punktu.

Ņemot vērā pieaugošos kiberdrošības riskus un lai stiprinātu spēju preventīvi konstatēt apdraudējumus kibertelpā, aicinām Aizsardzības ministrijai sadarbībā:

- *ar CERT.LV, izstrādāt kritērijus, lai apzinātu iestādes, kurās obligāti ir jāizvieto CERT.LV drošības sensori;*
- *ar VARAM izstrādāt stratēģiju drošības sensoru plašākai uzstādīšanai un izmantošanai, to starp, izstrādāto stratēģiju salāgojot ar VARAM uzsākto iniciatīvu IKT konsolidācijai.*

2. Vai iestādes veic nepieciešamās darbības, lai nodrošinātu e-pakalpojumu un to atbalstošo IS darbības nepārtrauktību?

Vai ir noteiktas prasības sasniedzamajam IS un e-pakalpojumu pieejamības līmenim?

Nacionālā līmenī izmantotajām IS sasniedzamā IS pieejamības līmeņa noteikšana pamatā tiek atstāta iestādes ziņā. Izņēmumi – integrētās valsts IS un valsts IS savietotājs.

Saskaņā ar normatīvo aktu[76] integrētajām valsts IS ir jānodrošina IS pieejamības līmenis 98% gadā no sistēmai noteiktā darbības laika (ja citos normatīvajos aktos nav noteikts citādi), savukārt valsts IS savietotājam – 99% gadā no sistēmai noteiktā darbības laika. Revīzijā konstatēti gadījumi, kad integrēto valsts IS darbību regulējošos normatīvajos aktos vidējie IS pieejamības rādītāji ir noteikti līdz pat 0,53% zemāki nekā tie ir noteikti MK noteikumos, kas nosaka pamata prasību IS pieejamības nodrošināšanai.

Lai gan normatīvais akts nosaka, ka e-pakalpojumiem ir jānodrošina pieejamība 98% mēnesī, tomēr tiem nav noteikts pakalpojuma sniegšanas laiks un netiek skaidrots, kādā laikā (iestādes

darba laiks vai 24/7 darbības režīms) ir jāsasniedz noteiktais e-pakalpojuma pieejamības līmenis, tādējādi jau valstiskā mērogā ir radīts maldīgs priekšstats, ka iestādes e-pakalpojums ir pieejams jebkurā dienā un jebkurā diennakts laikā.

Izmitinot e-pakalpojumu portālā Latvija.lv, tā pieejamība ir iespējama vienīgi portāla Latvija.lv uzturētāja VRAA noteiktajos un nodrošinātajos pieejamības laikos. Ņemot vērā, ka portāla pieejamība saskaņā ar normatīvo aktu prasībām ir jānodrošina vidēji 97,49% gadā, tiek radīts risks, ka iestādes, izmitinot e-pakalpojumus portālā Latvija.lv, nenodrošinās e-pakalpojumiem noteikto sasniedzamo pieejamības līmeni (98% mēnesī). Saskaņā ar revidenta aprēķiniem tas nozīmē, ka iestādes e-pakalpojums var tikt nodrošināts par gandrīz četrām stundām mēnesī mazākā apjomā, nekā paredz normatīvajā aktā[77] noteiktais pieejamības pamatlīmenis. Šis apstāklis rada risku, ka nesaskaņotu normatīvo prasību dēļ iespējams katru mēnesi var tikt radīts administratīvais slogs līdz pat 64 tūkst. *euro*[78]. Tā kā normatīvais regulējums, kas nosaka prasības e-pakalpojumu un portāla Latvija.lv pieejamībai ir spēkā kopš 2017.gada, secināms, ka piecu gadu laikā iespējams kopumā ir radītas administratīvā sloga izmaksas 3,84 milj. *euro* apmērā, kuras iedzīvotāji vai valsts pārvalde varēja izmantot citādāk. Ne visām nacionālā līmeņa IS, kas apmainās ar datiem ar citu valstu IS, sasniedzamo IS pieejamības līmeni (no 95% līdz 99,99% gadā no sistēmai paredzētā darba laika) ir noteikusi ES/EEZ. No tām 12 (kopumā 24), kurām ES/EEZ IS pieejamības līmeni ir noteikusi, deviņos gadījumos sasniedzamais IS pieejamības līmenis ir noteikts lielāks nekā 98% gadā, kas pārsniedz Latvijas normatīvajos aktos noteikto prasību 98% gadā integrētajām valsts IS un e-pakalpojumiem.

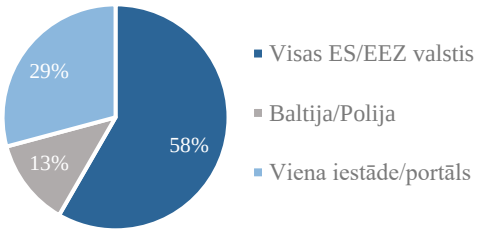
Starptautiskā līmenī noteiktās prasības sasniedzamajam IS pieejamības līmenim sistēmām, kas apmainās ar datiem ar citu valstu IS

Ekonomiskās sadarbības un attīstības organizācijas (*OECD*) ziņojumos un ES plānošanas un darbības pārskata dokumentos nav publicēta informācija par sasniedzamo pieejamības līmeni nacionālā līmeņa IS, kas apmainās ar datiem ar citu valstu IS, kā arī nav sniegta informācija par veiktiem pētījumiem saistībā ar nacionālā līmeņa IS sasniegto pieejamības līmeni, tomēr dokumentos ir uzsvērts IS pieejamības nozīmīgums. Piemēram, Eiropas Komisijas pārskatā[79] par ES dalībvalstu muitas sistēmu darbību 2020.gadā ir norādīts, ka ES dalībvalstu muitas IS darbības traucējumi ietekmē attiecīgās valsts muitas iestādes administrācijas darbu, iedzīvotājus un uzņēmumus visā ES un rada traucējumus ES iekšējā tirgū.

Atsevišķas nozares regulējošās ES regulās ir noteikts gan sasniedzamais IS pieejamības līmenis, gan IS darba laiks pašas ES uzturētajām IS un platformām, gan nacionālā līmeņa IS, kas apmainās ar datiem ar citas valsts IS ES mērogā. Piemēram, datu apmaiņai starp ES dalībvalstu muitas IS un nodokļu IS noteikts[80] 99,9% sasniedzamais IS pieejamības līmenis.

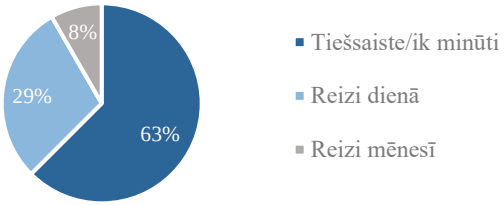
Saskaņā ar aptaujas rezultātiem par IS, kas apmainās ar datiem ar citu valstu IS, valsts pārvaldē tiek uzturētas vismaz 24 IS, kas ir nozīmīgas arī starptautiskā līmenī, nodrošinot informācijas apmaiņu ar citām valstīm, no tām:

- attiecībā uz datu apmaiņas tvērumu – 58% gadījumu (14 gadījumos no 24) datu apmaiņa tiek nodrošināta ar visām ES/EEZ dalībvalstīm (11.attēls); 29% gadījumu datu apmaiņa tiek veikta tikai starp atsevišķām organizācijām; 3 gadījumos – tikai Polijas un Baltijas valstu ietvaros;



11.attēls. Datu apmaiņas tvērums starp Latvijas IS un citu valstu IS

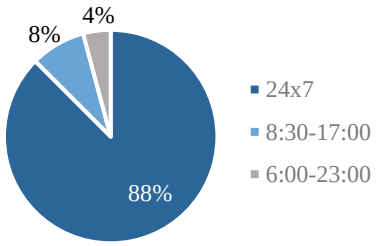
- attiecībā uz datu apmaiņas biežumu – 63% gadījumu (15 gadījumi no 24) datu apmaiņa tiek nodrošināta tiešsaistē jeb nekavējoties pēc pieprasījuma (datu apmaiņas intervāls nepārsniedz 1 minūti) (12.attēls);



12. attēls. Datu apmaiņas intervāli starp IS

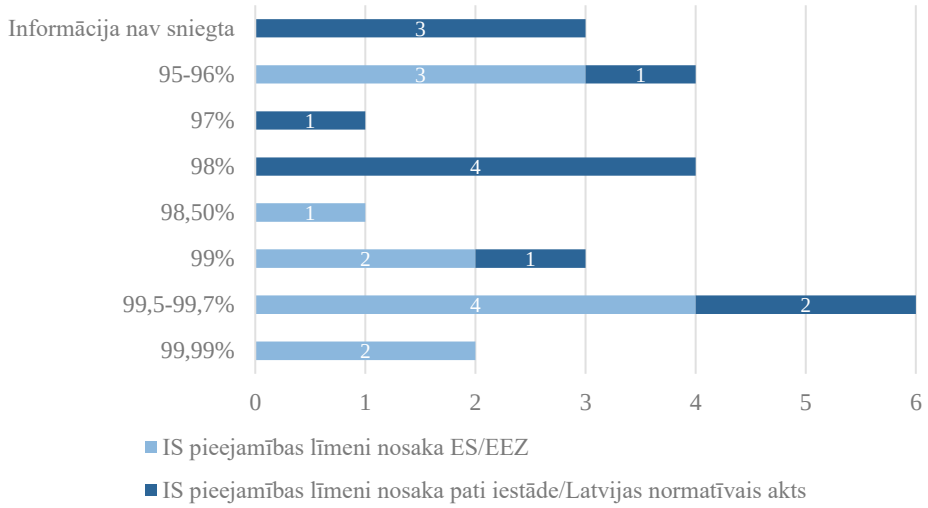
- pusē gadījumu (12 gadījumi jeb 50%) IS bez datu apmaiņas nodrošina arī kāda e-pakalpojuma sniegšanu. Šādi e-pakalpojumi ir saistīti ar informatīva rakstura datu un statistikas publicēšanu/iegūšanu, izziņu iegūšanu, kuģu satiksmes datu nodošanu, vīzu pieteikumiem, deklarāciju aizpildīšanu un datu pārbaudi/kontroli tālāku darbību veikšanai;

- attiecībā uz IS darba laika prasības izvirzīšanu – 88% gadījumu (21 gadījumā no 24) IS darba laiks ir noteikts 24 stundas 7 dienas nedēļā (13.attēls).
  Pusē gadījumu (12 gadījumi jeb 50%) IS darba laiku nosaka ES/EEZ prasības, bet pusē gadījumu to nosaka iestāde patstāvīgi (11 gadījumi jeb 46%) vai normatīvais akts (1 gadījums).



13.attēls. IS noteiktie darba laiki

- attiecībā uz IS pieejamības prasību izvirzīšanu – kopumā ES/EEZ vai iestādes pašas ir izvirzījušas sasniedzamo IS pieejamības līmeni robežās no 95% līdz 99,99% (14.attēls):



14.attēls. Nacionālā līmeņa IS, kuru pieejamība ir nozīmīga starptautiskajā līmenī, noteiktais sasniedzamais IS pieejamības līmenis

Tām IS, kurām ES/EEZ ir centralizēti noteikusi sasniedzamo IS pieejamības līmeni, sasniedzamais IS pieejamības līmenis tikai 3 gadījumos izvirzīts zemāks nekā 98%. Pārējos gadījumos (9 IS) sasniedzamais IS pieejamības līmenis noteikts no 98,5% līdz pat 99,99%.

Nacionālā līmenī noteiktais sasniedzamais pieejamības līmenis informācijas sistēmām

Normatīvais akts, kurā noteikta kārtība, kādā tiek nodrošināta IKT sistēmu atbilstība minimālajām drošības prasībām, nosaka, ka IS valstī iedala divās kategorijās – pamata un paaugstinātas drošības sistēmas[81]. Konkrēts sasniedzamais IS pieejamības līmenis atkarībā no drošības kategorijas nav noteikts.

Normatīvais akts[82] konkrētu sasniedzamo pieejamības līmeni nosaka tikai integrētajām valsts IS un valsts IS savietotājam:

- integrētajai valsts IS (tā ir IS, kas apmainās ar datiem ar citu valsts IS) pieejamība jānodrošina vismaz 98% apjomā (gadā) no sistēmai noteiktā darbības laika;
- savietotāja (IS, kas nodrošina centralizētu datu apmaiņas punktu starp valsts IS) pieejamība jānodrošina vismaz 99% apjomā (gadā) no savietotājam noteiktā darbības laika.

Normatīvais akts nenosaka, kāds integrētajām valsts IS ir nosakāmais darbības laiks (atbilstoši iestādes darba laikam vai 24/7 darba laikam), lai gan no tā ir atkarīgs, kādā laikā pieejamības līmenis ir jāsasniedz. Sistēmas darbības laiku izvēlas un nosaka iestādes.

Savukārt VRAA uzturētajam valsts IS savietotājam normatīvais akts[83] nosaka darba laiku 24 stundas diennaktī (5.tabula).

5.tabula

IS darba laiks un normatīvajā aktā noteiktais sasniedzamais IS pieejamības līmenis

	Sasniedzamais IS pieejamības līmenis	
	Pamata drošības kategorijas IS	Paaugstinātas drošības kategorijas IS
Iestādē izmantotās IS **Valsts IS***	Iestāde pati nosaka sasniedzamo IS pieejamības līmeni un IS darbības laiku	
Integrētās valsts IS*	98% apjomā (gadā) no savietojamās sistēmas noteiktā darbības laika, ko nosaka iestāde	
Valsts IS savietotājs	99% apjomā (gadā) 24/7 darbības režīmā	

* ja citos normatīvajos aktos nav noteikts citādi

Atsevišķos gadījumos valsts IS darbības noteikšanai ir izstrādāti normatīvie akti, kuros ir noteikts arī sasniedzamais IS pieejamības līmenis. Revīzijas apjomā iekļautās deviņas iestādes uztur 38 valsts IS. No tām 19 IS ir izstrādāti Ministru kabineta noteikumi, kas nosaka informācijas apstrādi tajās, bet ne visos gadījumos ir paredzēts sasniedzamais IS pieejamības līmenis. Tas ir noteikts tikai piecos gadījumos (6.tabula).

6.tabula

[IP]

[IP]

Jānorāda: gadījumos, ja ir izstrādāti atsevišķi Ministru kabineta noteikumi, kas nosaka informācijas apstrādi specifiskās IS, šajos Ministru kabineta noteikumos norādītie sasniedzamie IS pieejamības rādītāji var tikt noteikti zemāki nekā pamatregulējumā noteiktais sasniedzamais IS pieejamības līmenis. Revīzijā izvērtētajos gadījumos konstatētā atšķirība veidojas no IS pieejamības diferencēšanas atkarībā no IS noteiktā darba laika. Revidentu veiktais aprēķins rāda, ka gada ietvaros, diferencējot IS pieejamību pret iestādes darba laiku un ārpus iestādes darba laiku, netiek sasniegta vispārējos noteikumos noteiktā 98% pieejamība gadā (skatīt 6.tabulu).

Nacionālā līmenī noteiktais sasniedzamais pieejamības līmenis e-pakalpojumiem

Saskaņā ar normatīvo aktu[90]:

- iestāde ir atbildīga par e-pakalpojuma plānošanu, nodrošināšanu, uzturēšanu un attīstību, kā arī nodrošina e-pakalpojuma darbības vides pieejamību e-pakalpojuma saņēmējam;
- iestādei ir jānodrošina e-pakalpojuma darbspējas (jeb pieejamības) laiks 98% mēnesī. Nav noteikts kādā laikā – iestādes darba laikā vai 24/7 darbības režīmā – ir jāsasniedz normatīvajā aktā noteiktais e-pakalpojuma pieejamības līmenis.

Izmitinot e-pakalpojumu portālā Latvija.lv, iestāde piekrīt VRAA iekšējiem noteikumiem[91], saskaņā ar kuriem VRAA nodrošina pakalpojumu pieejamību šādā apjomā:

- darba dienās darba laikā no 8.30 līdz 17.00 – 99 % mēnesī no VRAA risinājumu koplietošanas pakalpojumu sniegšanas laika;
- pārējā laikā – 97 % mēnesī no VRAA risinājumu koplietošanas pakalpojumu sniegšanas laika.

E-pakalpojumu izmitinot portālā Latvija.lv, tā pieejamība ir atkarīga ne tikai no iestādes IS darbības, bet arī no portāla un autentifikācijas risinājumu pieejamības. Ņemot vērā, ka kopumā portāla Latvija.lv pieejamība ir jānodrošina vidēji 97,49% gadā[92], iestādes, izmitinot e-pakalpojumus portālā Latvija.lv, nesasniegs e-pakalpojumiem noteikto pieejamības līmeni, t.i., 98% mēnesī (skatīt 7.tabulu).

Saskaņā ar revidenta aprēķiniem tas nozīmē, ka iestādes e-pakalpojums var tikt nodrošināts par gandrīz četrām stundām mēnesī mazākā apjomā, nekā paredz vispārējais pamatregulējums e-pakalpojuma pieejamībai. Ņemot vērā, ka administratīvais slogs vienas stundas nepieejamībai portālam Latvija.lv var būt līdz pat 16 tūkst. *euro*, secināms, ka nesaskaņotu normatīvo prasību dēļ katru mēnesi var tikt radīts administratīvais slogs līdz pat 64 tūkst. *euro*[93]. Tā kā normatīvais regulējums, kas nosaka prasības e-pakalpojumu un portāla Latvija.lv pieejamībai ir spēkā kopš 2017.gada, tādejādi secināms, ka piecu gadu laikā valstiski iespējams ir radīts administratīvais slogs 3,84 miljoni *euro*.

7.tabula

Revidenta aplēse e-pakalpojumu izpildē iesaistīto IS un resursu nodrošināmās pieejamības atšķirībām

Normatīvais akts		Stundas gadā*	Noteiktais IS pieejamības līmenis	Revidentu aplēstās darba stundas (gadā)	Atšķirība pret vispārējo regulējumu
Vispārējā prasība e-pakalpojumam (MK402)		**8760 h**	**98% mēnesī**	**8585 h**	**x**
Valsts pārvaldes pakalpojumu portāls (VRAA) (MK400)	Iestādes darba laikā 8.30–17.00	2142 h	99% gadā	2121 h	**-45**
	Ārpus iestādes darba laika un brīvdienās	6618 h	97% gadā	6419 h	
eParaksta IS (MK560)	Darbdienās 9.00–18.00	2268 h	99,5% gadā	2257 h	**-31**
	Pārējā laikā	6492 h	97% gadā	6297 h	

*2021.gadā ir 365 dienas (no tām 252 darba dienas)=24h*365 dienas = 8760h.

Turklāt, ņemot vērā, ka normatīvais akts[94] nenosaka, kādā laikā – iestādes darba laikā vai 24/7 darbības režīmā – ir jāsasniedz noteiktais e-pakalpojuma pieejamības līmenis, pakalpojumu saņēmējiem jau valstiskā mērogā tiek radīts maldīgs priekšstats, ka iestādes e-pakalpojums ir pieejams jebkurā dienā un jebkurā diennakts laikā.

Ieteikums

Lai nodrošinātu savstarpēji saskaņotas prasības IS un e-pakalpojumu noteiktajam darbības laikam un sasniedzamajam pieejamības līmenim, VARAM pārskatīt normatīvos aktus un nodrošināt savstarpējo saikni starp prasībām portāla Latvija.lv pieejamībai, e-pakalpojumu pieejamībai un darbības laikam.

Vai iestādēs ir ieviesti priekšnoteikumi IS pieejamības nodrošināšanai?

Normatīvajā aktā[95] (t.sk. labajā praksē[96]) ir ietverti priekšnoteikumi, kuru izpilde ir nepieciešama, lai iestādēs sekmētu IS pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktību. Ne visi normatīvajā aktā ietvertie priekšnoteikumi IKT darbības nepārtrauktības un IS pieejamības nodrošināšanai ir jāattiecina uz visām iestādē izmantotajām IS. Piemēram, ja iestādē tiek izmantotas pamata drošības IS, tad šīm sistēmām nav jāizstrādā šāda dokumentācija: IS drošības risku novērtējums, IS drošības risku pārvaldības plāns un IS darbības atjaunošanas plāns. Tomēr pamata prasība – iestāde nodrošina datu rezerves kopiju veidošanu un datu rezerves kopiju atjaunošanu – ir noteikta gan pamata, gan paaugstinātas drošības IS. No tā izriet, ka datu atjaunošana iestādei ir jānodrošina arī gadījumā, ja iestāde nav izstrādājusi dokumentāciju rezerves kopiju veidošanai, glabāšanai un atjaunošanai.

Lai gan visās deviņās revīzijas apjomā iekļautajās iestādēs tiek uzturētas paaugstinātas drošības IS, nevienā no tām nav ieviesti visi priekšnoteikumi pilnībā. Biežākās problēmas ir saistītas ar to, ka iestādes (trīs iestādes) plānošanas dokumentos nav iestrādāts mērķis IS pieejamības nodrošināšanai. Nenosakot mērķus un uzdevumus IS pieejamības nodrošināšanai, IS pieejamība nav apzināta kā būtiska nepieciešamība iestādes funkciju nodrošināšanai.

Tāpat konstatēti trūkumi IS darbības atjaunošanas plāna izstrādē (trijās iestādēs nav izstrādāts vispār) un IS drošības risku izvērtēšanā (divās iestrādēs nav veikts vispār). Šie ir būtiski priekšnoteikumi, kuru trūkums liecina par vāju kontroles vidi iestādes spējai īsā laikā nodrošināt IS pieejamības atjaunošanu.

Lai gan piecās iestādēs ir apzināti IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas ir būtiski iestādes funkciju izpildes atbalsta nodrošināšanā, tomēr pārējās četrās iestādēs būtiskie IKT resursi ir identificēti daļēji, piemēram, identificējot tikai IS. Tādējādi visas izrietošās nepārtrauktības plānošanas darbības ir orientētas tikai uz IS darbības nepārtrauktības plānošanu, kas ir tikai daļa no darbības nodrošināšanā iesaistītajiem IKT resursiem. Turklāt incidentu gadījumā (IKT infrastruktūras vai sakaru pakalpojumu bojājuma gadījumā) iestāde nespēs pietiekami ātri reaģēt un novērst problēmas ar IS nesaistītos resursos.

Vērtējot iestāžu noslēgto līgumu par IS uzturēšanas darbu nodošanu ārpakalpojuma sniedzējam noteikumus, konstatēts, ka tajos iekļautās IS pieejamības prasības ir vispārīgas un nenosaka sasniedzamo IS pieejamības līmeni, radot risku, ka normatīvajā aktā noteiktais IS pieejamības līmenis ārpakalpojumā nodotajām IS netiks sasniegts, tādejādi ārpakalpojumā nodotajām sistēmām neveicinot valsts pārvaldē kopumā noteiktā pieejamības līmeņa sasniegšanu.

Labā prakse un normatīvais akts nosaka vairākus priekšnoteikumus[97], kuru izpilde ir nepieciešama, lai iestādēs sekmētu IS un ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanu. Jānorāda, ka ne visi normatīvajā aktā ietvertie priekšnoteikumi IKT darbības nepārtrauktības un IS pieejamības nodrošināšanai ir jāattiecina uz visām iestādē izmantotajām IS. Piemēram, ja iestādē tiek izmantotas pamata drošības IS, tad šīm sistēmām nav jāizstrādā šāda dokumentācija: IS drošības risku novērtējums, IS drošības risku pārvaldības plāns un IS darbības atjaunošanas plāns. Tomēr pamata prasība – iestāde nodrošina datu rezerves kopiju veidošanu un datu rezerves kopiju atjaunošanu – ir noteikta[98] gan pamata, gan paaugstinātas drošības kategorijas IS. No tā izriet, ka datu atjaunošana iestādei ir jānodrošina arī gadījumā, ja iestāde nav izstrādājusi dokumentāciju rezerves kopiju veidošanai, glabāšanai un atjaunošanai.

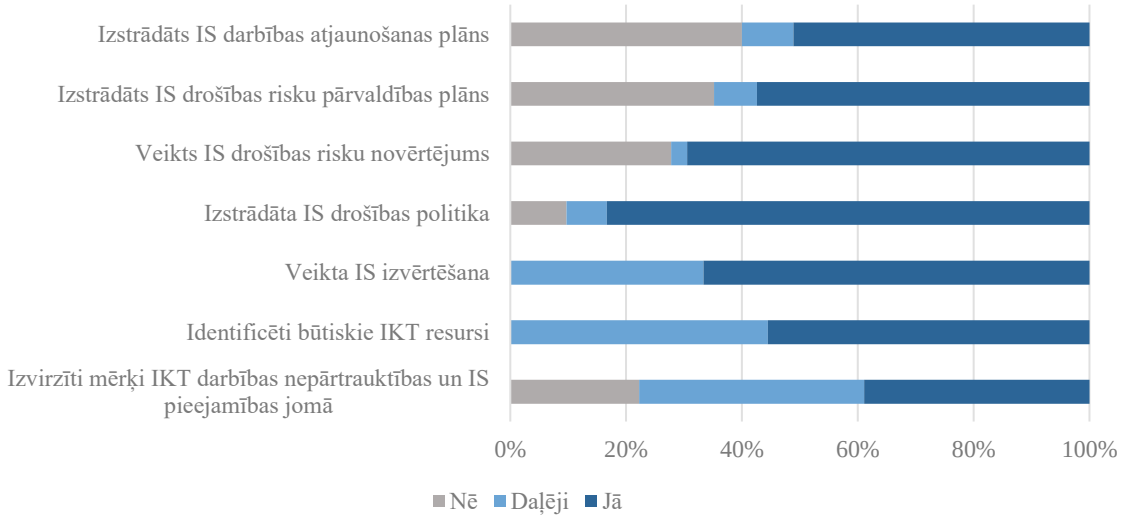
Lai revīzijā salīdzinātu iestādēs ieviestos priekšnoteikumus IS pieejamības un IKT darbības nepārtrauktības nodrošināšanai, revidenti izveidoja pārbaudes lapu, tajā iekļaujot labās prakses[99] un normatīvajā aktā[100] ietvertos priekšnoteikumus, kas paredz, ka iestādē ir:

- izvirzīts mērķis IKT darbības nepārtrauktībai un sasniedzamajai IS pieejamībai (piemēram, iestādē ir izstrādāts dokuments (stratēģija, IKT darbības politika vai cita veida dokuments) ar ietvertiem mērķiem IKT darbības nepārtrauktības nodrošināšanā);
- apzināti būtiskie IKT resursi, kas ir iesaistīti iestādes funkciju izpildes atbalsta nodrošināšanā;
- saskaņā ar normatīvo aktu izvērtētas IS, tās nodalot pamata vai paaugstinātas drošības kategorijā (revīzijā iesniegtais iestādes izvērtējums sakrīt ar VIRSIS norādīto informāciju);
- izstrādāta IS drošības politika, tā tiek pārskatīta reizi gadā vai līdz ar būtiskām IS darbības un konfigurācijas izmaiņām vai pēc nozīmīgiem drošības incidentiem. IS drošības politika ietver:
  - sistēmas drošības politikas mērķus un pamatnostādnes;
  - sistēmas raksturojumu un analīzi drošības jomā;
  - sistēmas drošības pārvaldības organizācijas principus;
  - sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;
  - sistēmas drošības principus, sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamo līmeni;
  - nosacījumus, kad ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām.
- veikts IS drošības risku novērtējums atbilstoši normatīvajā aktā paredzētajiem nosacījumiem – iestādē ir izstrādāta IS drošības risku analīze, IS drošības risku analīzē ietverts būtisko IKT resursu un IS risku izvērtējums, IS drošības risku analīze tiek pārbaudīta un atjaunota reizi gadā vai līdz ar būtiskām IS darbības un konfigurācijas izmaiņām, vai pēc nozīmīgiem drošības incidentiem. IS drošības risku analīze ietver:
  - sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu;
  - institūcijas, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu sistēmas drošības incidents;
  - sistēmas drošības riska novērtējumu;
  - sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu;
  - sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.

- izstrādāts IS drošības risku pārvaldības plāns, IS drošības risku pārvaldības plāns izstrādāts un aktualizēts, pamatojoties uz IS drošības risku analīzi, IS drošības risku pārvaldības plāns tiek pārbaudīts un atjaunots reizi gadā vai biežāk, ja ir bijušas būtiskas IS darbības un konfigurācijas izmaiņas vai pēc nozīmīgiem drošības incidentiem, kā arī vai IS drošības risku pārvaldības plāns ietver:
  - veicamās risku analīzes metodoloģijas aprakstu;
  - sistēmas drošības risku analīzi;
  - pasākumus sistēmas drošības riska mazināšanai, to izpildes termiņus, finansējumu un par izpildi atbildīgo personu sarakstu;
- izstrādāts IS darbības atjaunošanas plāns un plāns ietver:
  - sistēmas IKT resursu atjaunošanas pasākumus, kas veicami pēc sistēmas drošības incidenta;
  - IS darbības atjaunošanas pasākumu procedūru aprakstu;
  - IS darbības atjaunošanas pasākumos iesaistīto atbildīgo personu apziņošanas kārtību un darbības instrukcijas;
  - atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.

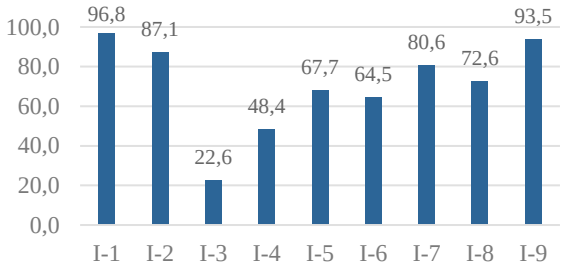
Revīzijā, izvērtējot situāciju deviņās iestādēs, kas uztur paaugstinātas drošības kategorijas IS, konstatēts, ka:

- biežākās problēmas ir saistītas ar to, ka iestādes plānošanas dokumentos nav iestrādāts mērķis IS pieejamības nodrošināšanai, trūkumiem IS darbības atjaunošanas plānā un IS drošības risku izvērtēšanā (15.attēls);



15.attēls. Iestādēs ieviesto kritēriju īpatsvars (%) IS pieejamības un IKT darbības nepārtrauktības nodrošināšanai

- tikai četrās no deviņām revīzijā vērtētajām iestādēm ir ieviesti vismaz 80% no revidentu apzinātajiem priekšnoteikumu kritērijiem IS pieejamības nodrošināšanai (16.attēls). Divās iestādēs ir ieviesta ne vairāk kā puse šo priekšnoteikumu, radot risku vājai kontroles videi šo iestāžu IS darbības nodrošināšanai un atjaunošanai;



16.attēls. Iestādēs ieviestie priekšnoteikumi (kritēriju īpatsvars procentos) IS pieejamības nodrošināšanai

- tikai trijās iestādēs IKT darbības nepārtrauktības un IS pieejamības jautājumi ir ietverti iestādes darbības vai IKT stratēģijās, kā arī pakārtotajos darbu plānos, pārējās sešās iestādēs, nenosakot mērķus un uzdevumus IS pieejamības nodrošināšanai, IS pieejamība nav apzināta kā būtiska nepieciešamība iestādes funkciju nodrošināšanai;
- piecās iestādes ir apzināti IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas ir būtiski iestādes funkciju izpildes atbalsta nodrošināšanā, tomēr pārējās četrās iestādēs būtiskie IKT resursi ir identificēti daļēji, piemēram, identificējot tikai IS.

  Tādējādi visas izrietošās nepārtrauktības plānošanas darbības ir orientētas tikai uz IS darbības nepārtrauktības plānošanu, kas ir tikai daļa no darbības nodrošināšanā iesaistītajiem IKT resursiem. Turklāt incidentu gadījumā (IKT infrastruktūras vai sakaru pakalpojumu bojājuma gadījumā) iestāde nespēs pietiekami ātri reaģēt un novērst problēmas ar IS nesaistītos resursos.
- trīs iestādēs nav izstrādāts IS drošības risku pārvaldības plāns;
- divās iestādēs nav veikts IS drošības risku izvērtējums;
- trijās iestādēs nav izstrādāts IS darbības atjaunošanas plāns;
- lai gan kopumā iestādes ir izvērtējušas uzturētās IS, tomēr revidentu ieskatā vairākas valsts IS, kas pašlaik reģistrētas VIRSIS kā pamata drošības IS, būtu nosakāmas kā paaugstinātas drošības IS (detalizēti skatīt ziņojuma projekta sadaļu "Vai vienkopus ir apzinātas valstī izmantotās IS?").

Iestādes ne tikai pašas var uzturēt IS, bet tās var nodot izmitināšanā un uzturēšanā arī ārpakalpojuma sniedzējam. Piemēram, iestādes var izmantot LVRTC pakalpojumus[101] datu rezerves kopēšanai vai sava resora koplietošanas IKT pakalpojumu sniedzēja nodrošinātos pakalpojumus (piemēram, iekšlietu resorā – Iekšlietu ministrijas Informācijas centrs, tieslietu resorā – VAS "Tiesu nama aģentūra", labklājības resorā – Valsts sociālās apdrošināšanas aģentūra u.c.).

Normatīvais akts nosaka[102], ka institūcija, sistēmas uzturēšanai slēdzot ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līgumā nosaka:

- saņemamā ārpakalpojuma aprakstu;
- precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;
- iestādes un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā institūcijas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti un institūcijas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi.

Revīzijā konstatēts, ka četras no deviņām revīzijas apjomā iekļautajām iestādēm ir noslēgušas ārpakalpojuma līgumus par iestādes IS vai ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanu, bet nevienā no tiem nav ietvertas detalizētas prasības IS un ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanai un ziņošanai par faktiski sasniegto pieejamības līmeni.

Piemēram, līgumā starp iestādi un ārpakalpojuma sniedzēju ir noteikts iestādes IS darbības laiks (darba laiks), bet nav noteikts pieejamības līmenis, kas ārpakalpojuma sniedzējam ir jānodrošina. Sasniedzamais IS pieejamības līmenis nav līgumā noteikts, lai gan normatīvais akts[103] izvirza, piemēram, integrētajām valsts IS nodrošināt pieejamības līmeni 98% gadā.

Vai iestādēs ir ieviesti risinājumi IS un e-pakalpojumu pieejamības uzraudzībai?

Iestādēs izmantotajām IS (ja vien tās nav integrētās valsts IS vai savietotājs) normatīvajos aktos nav noteikti tehniskie risinājumi, kurus ieviešot iestāde nodrošina savu IS darbību un sekmē noteiktu IS pieejamības līmeņa sasniegšanu. Atbilstošu tehnisko risinājumu IS pieejamības līmeņa nodrošināšanai, tai skaitā IKT infrastruktūras, izvēle un kritēriji IS darbības nepārtrauktības uzraudzībai ir katras iestādes pārziņā.

Normatīvie akti izvirza prasības tikai integrēto valsts IS un savietotāja tehniskās darbības nodrošināšanai, tomēr minētās prasības vairāk ir attiecināmas uz tehniskajiem risinājumiem IKT infrastruktūras darbības nepārtrauktības nodrošināšanai, nevis konkrēta IS pieejamības līmeņa sasniegšanai. Izvirzītās prasības nenoliedzami sekmē arī IS pieejamības līmeņa nodrošināšanu, tomēr to izpilde pati par sevi negarantē, ka iestāde sasniegs IS (t.sk. e-pakalpojumu) pieejamības līmeni.

Nevienā nacionāla līmeņa normatīvajā aktā vai vadlīnijās nav noteikti kritēriji IS un e-pakalpojumu funkcionālajai un pieejamības uzraudzībai. Revidentu ieskatā vienlaikus ar tehnisko prasību izvirzīšanu IKT infrastruktūras darbības nepārtrauktības nodrošināšanai ir jānosaka uzraugāmi kritēriji IS un e-pakalpojumu pieejamības kontrolei, kurus regulāri uzraugot ir iespējams gūt pārliecību, vai IS un e-pakalpojumi ir bijuši pieejami.

Ņemot vērā, ka normatīvajos aktos nav noteikti vai vadlīnijās aprakstīti kritēriji, kurus uzraugot iestāde varētu gūt viennozīmīgu pārliecību par to, ka tās IS ir pieejama, kā arī nav skaidra normatīvajos aktos lietotā terminoloģija, kas saistāma ar IS darba laika un pieejamības noteikšanu, iestāžu patstāvīgi izvēlētie un ieviestie organizatoriskie un tehniskie pasākumi IS pieejamības pārvaldībai var būt nepietiekami un nesniedz patiesu priekšstatu par sasniegto IS pieejamības līmeni iestādēs.

Bez tā, ka normatīvajos aktos nav noteikti uzraugāmie kritēriji IS un e-pakalpojumu pieejamības, kā arī IKT infrastruktūras darbības nepārtrauktības kontrolei, iestādēm trūkst vienotu, aktuālu, valsts līmenī pārskatītu un patstāvīgai piemērošanai pieejamu vadlīniju vai metodikas IS un e-pakalpojumu pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktības novērtēšanai. Lai gan starptautiskā mērogā ir pieejamas dažādas vadlīnijas, standarti un metodikas, galvenokārt IS drošības jomā, kas ietver arī IS pieejamības un IKT darbības nepārtrauktības jautājumus, tomēr revidentu ieskatā būtu nepieciešamas VARAM un AiM apkopotas, izvērtētas un Latvijas videi pielāgotas vadlīnijas, lai iestādes mērķtiecīgi ieviestu organizatoriskos un tehniskos pasākumus, kā arī lai īstenotu IS pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktības pārvaldību. Būtiski arī, lai vadlīnijās tiktu paskaidrota normatīvajos aktos esošā terminoloģija, kas saistāma ar IS darba laiku un pieejamību, kā arī ietverta metodika, kā būtu aprēķināma faktiskā IS pieejamība, tai skaitā – kādus parametrus ņemt vai neņemt vērā, nosakot sasniegto IS un e-pakalpojumu pieejamības līmeni.

Revīzijas apjomā iekļautās iestādes nodrošina IKT infrastruktūras darbību ietekmējošo elementu uzraudzību, kā arī nodrošina IKT infrastruktūras darbības uzraudzību, tomēr lielākā daļa no revīzijas apjomā iekļautajām iestādēm (septiņas no deviņām) ir norādījušas, ka to rīcībā nav tādu rīku, kas veiktu IS un e-pakalpojumu funkcionālo uzraudzību – attiecīgi šajās iestādēs no deviņām netiek nodrošināta pilnā apmērā IS un e-pakalpojumu darbības uzraudzība. Ņemot vērā, ka iestādes nodrošina IKT infrastruktūras darbības uzraudzību, bet nenodrošina pilnā apmērā IS un e-pakalpojumu darbības uzraudzību, tiek radīts risks, ka IKT infrastruktūra un uz tās darbojošās IS komponentes var darboties, bet tai pašā laikā IS funkcionalitāte vai e-pakalpojums var darboties nepilnvērtīgi vai nedarboties vispār.

Normatīvajos aktos nav noteikti un vadlīnijās nav skaidroti kritēriji, kas jāmēra un kurus uzraugot iestāde varētu gūt viennozīmīgu pārliecību par to, ka IS un e-pakalpojums ir pieejami. Normatīvajos aktos noteiktās prasības iestādē nepieciešamajai dokumentācijai un rīcībai IS darbības atjaunošanas plānošanai un atjaunošanai ir priekšnoteikumi, kuru izpilde ir nepieciešama, lai iestādēs sekmētu IS pieejamību. Šo priekšnoteikumu izpilde negarantē to, ka IS un e-pakalpojumi darbosies ar noteiktu pieejamības līmeni. Iestādes pašas izvēlas un nosaka, kādā veidā monitorēt IS un e-pakalpojumu pieejamību, tostarp – kādus parametrus izvirzīt un ikdienā uzraudzīt.

Prasību darbības nepārtrauktībai noteikšana normatīvajos aktos pati par sevi nevar nodrošināt, ka IS un e-pakalpojumi darbosies ar noteiktu pieejamības līmeni. Vienlaikus nepieciešams mehānisms, kā nodrošināt uzraudzību praktiski, lai pārliecinātos, vai IS un e-pakalpojumi ir pieejami lietotājiem, vai IS strādā bez kļūdām, vai e-pakalpojums darbojas un to ir iespējams saņemt.

Bez tā, ka līdz šim normatīvajos aktos nav noteikti un vadlīnijās nav aprakstīti kritēriji, kurus uzraugot iestāde varētu gūt viennozīmīgu pārliecību par to, ka tās IS un e-pakalpojumi ir pieejami, trūkst arī norādījumu, kādu informāciju uzkrāt un kā izmērīt sasniegto IS pieejamību. Tostarp nav noteikts, pret ko attiecināt IS pieejamībai noteikto sasniedzamo līmeni (98% gadā) – pret iestādes darba laiku vai kalendāro dienu skaitu gadā. Metodika IS pieejamības aprēķināšanai ir būtiska, lai ne tikai iestāde apzinātu sasniegto IS pieejamību un vērtētu pret izvirzīto, bet arī e-pārvaldes pieejamības novērtēšanai kopumā. Turklāt iestāžu nodrošinātais IS pieejamības līmenis ir būtiska informācija, lai apzinātu problemātiskās e-pārvaldes jomas un plānotu nepieciešamo atbalstu.

Iestādes lielākoties uzrauga un vērtē kādu no komponentiem, kas ietekmē kopējo IS pieejamību, piemēram, IS datu bāzes pieejamību vai servera darbību, bet nemēra un nevērtē citu komponentu (piemēram, funkcionalitātes pieejamības rādītājus IS lietotājiem) pieejamību. Tādējādi tiek radīts risks, ka iestādēs nav korektas informācijas par sasniegto IS pieejamības līmeni, savukārt informatīvajiem mērķiem aprēķinātais IS pieejamības līmenis ir nekorekts, jo tajā tiek atspoguļota tikai viena komponenta sasniegtā pieejamība, kas neatspoguļo kopējo sasniegto IS vai e-pakalpojumu pieejamības līmeni.

Normatīvais akts[104] tikai integrētajām valsts IS un savietotājam nosaka, ka jānodrošina atbilstība normālam ekspluatācijas režīmam, veicot monitoringu dažādiem IS pieejamību ietekmējošiem parametriem, piemēram, uzraugot IKT resursu kritiskās robežas (procesora noslodze, RAM noslodze, datu kanālu noslodze) un IS veiktspējas rādītājus.

Normatīvajā aktā[105] noteiktie parametri IKT resursu kritisko robežu monitoringam faktiski ir attiecināmi uz IKT infrastruktūras darbības uzraudzību. Parametrus, kas ir saistīti ar IS un e-pakalpojumu pieejamību, normatīvie akti neparedz.

[IP]

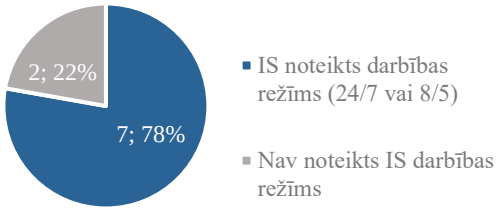
Attiecībā uz e-pakalpojumu pieejamības uzraudzību septiņas iestādes norādīja, ka to rīcībā nav tādu rīku. Tikai divās iestādēs ieviesti risinājumi, kas nodrošina IS un e-pakalpojumu pieejamības uzraudzību. [IP]

Risinājums uzkrāj informāciju par e-pakalpojumu pieejamību un sniedz pārskatus par rādītājiem dažādos periodos.

Metodika

Normatīvajos aktos nav noteikts konkrēts darba laiks e-pakalpojumu saņemšanai, un ne visos gadījumos to ir noteikusi iestāde. Arī portālā Latvija.lv nav norādīts e-pakalpojumu darba laiks. E-pakalpojuma darba laiks ir cieši saistīts un izriet no IS darba laika.

Revīzijā, apzinot IS noteikto darba laiku deviņās revīzijā apskatītajās iestādēs, konstatēts, ka divās iestādes nav noteikts IS darba laiks, septiņas iestādes noteikušas, ka IS darbojas 24/7 vai 8/5 režīmā, bet garantētais darba laiks tiek nodrošināts iestādes darba laikā (17.attēls).

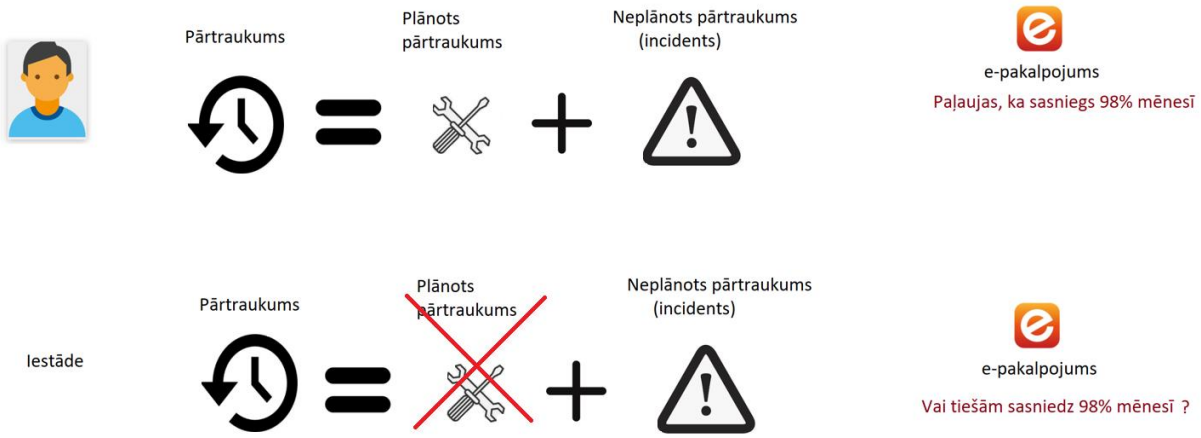


17.attēls. Iestādēs IS noteiktie darbības režīmi

Normatīvajos aktos[106] tiek lietoti vismaz trīs jēdzieni – "sistēmai paredzētais darba laiks", "sistēmai noteiktais darbības laiks", "sistēmas nepārtrauktās darbības laiks". Šie jēdzieni ir sasaistāmi ar IS darba laiku, bet tie nav pietiekami skaidri un viennozīmīgi piemērojami – vai tas ir IS darba laiks noteiktās dienās saskaņā ar iestādes darba laiku, vai IS darba laiks atbilst 24/7 darbības režīmam un nodrošina iespēju e-pakalpojumu saņemt neatkarīgi no iestādes darba laika, kāds ir IS darbības obligātais darba laiks, kurā e-pakalpojumam ir jābūt nodrošinātam un šajā laikā nedrīkst plānot IS darbības pārtraukumus.

Piemēram: iestādei jānodrošina[107] e-pakalpojumam pieejamība 98% mēnesī jeb 98% gadā. Ja iestāde ir noteikusi, ka sistēmai darbības laiks ir 24/7 jeb 8760 stundas gadā, lai sasniegtu 98% pieejamību, e-pakalpojums var nebūt pieejams līdz 175 stundām gadā (2%) jeb gandrīz četras stundas katru nedēļu. Ņemot vērā, ka iestāde nav noteikusi laiku, kad IS tiek veikta plānota nepieejamība, piemēram, uzturēšanas darbi, tad tie var tikt veikti iestādes darba laikā. Tā rezultātā faktiski IS un e-pakalpojumi var nebūt pieejami katru nedēļu iestādes darba laikā vismaz četras stundas.

Vērtējot, vai iestādēs ir noteikta metodika, kā aprēķināt sasniegto IS un e-pakalpojumu pieejamības līmeni, konstatēts, ka nav konkrētas aprēķina metodikas, kas balstās uz noteiktu rādītāju uzkrāšanu un vērtēšanu. Turklāt atsevišķas iestādes revīzijā informēja, ka plānotos IS uzturēšanas darbus IS pieejamības aprēķinā neietver, bet IS pieejamību attiecina tikai uz neplānotiem darbības pārtraukumiem. Piemēram, iestāde ir noteikusi, ka IS darbojas 24/7 režīmā un sistēmai pieļaujamas dīkstāves darba dienās laikā no 20.00 līdz 00.00, kuras netiks iekļautas pieejamības aprēķinā (18.attēls).



18.attēls. IS plānoto pārtraukumu ietveršana IS un e-pakalpojumu pieejamības aprēķinos – iedzīvotāja gaidas un iestādēs piemērotā prakse

Revidentu ieskatā šī pieeja ir korekta attiecībā uz to, ka iestāde plāno uzturēšanas darbus veikt nakts laikā, lai mazāk ietekmētu privātpersonu loku, kas pakalpojumu gribētu saņemt. Tomēr, IS dīkstāves laiku neietverot aprēķinā vispār, rodas maldīgs priekšstats par sasniegto pieejamības līmeni, kas vēl vairāk pastiprina nepieciešamību izstrādāt metodiku, kā aprēķināt sasniegto pieejamības līmeni, detalizēti nosakot, vai to attiecināt uz IS darbības laiku saskaņā ar iestādes darba laiku vai 24/7 darbību.

Ieteikums

Lai iestādēs nodrošinātu vienotu pieeju, VARAM izstrādāt metodiku IS un e-pakalpojumu pieejamības aprēķināšanai, tai skaitā nosakot, kādus rādītājus uzkrāt IS un e-pakalpojumu pieejamības aprēķinam un pret ko tos attiecināt.

Vai iestāde spēs atjaunot IS pieejamību incidentu gadījumos?

No tām sešām revīzijā vērtētajām iestādēm, kuras bija izstrādājušas IS atjaunošanas plānu, trijās nav veiktas plāna atbilstības pārbaudes IS pieejamības atjaunošanai, kas samazinātu risku, ka incidentu gadījumā nevarēs nodrošināt IKT darbības un IS pieejamības atjaunošanu pietiekami īsā laikā vai vispār. Iestādēs izstrādātie IS darbības atjaunošanas plāni nav testēti, pārbaudot plānu pilnīgumu, proti, vai saskaņā ar plānu, pieejamiem tehniskajiem resursiem, uzglabātajām rezerves kopijām un darbinieku kompetenci IS pieejamība ir atjaunojama iestādē noteiktajā laikā.

Iestādes galvenokārt paļaujas uz rezerves kopiju veidošanai iebūvētajām kontrolēm, kuras rezerves kopiju izveides brīdī ziņo, vai kopija izveidota un vai tā ir izveidota bez kļūdām. Datu atjaunošanas pārbaudi no rezerves kopijas rezerves kopēšanas sistēma neveic, līdz ar to iestāžu paļaušanās tikai uz rezerves kopēšanas sistēmas ziņojumiem par kopijas izgatavošanas faktu, bet praktiskas IS datu atjaunošanas pārbaudes neveikšana ir pretrunā normatīvajā aktā[108] noteiktajam, ka integrētajām valsts IS testa vidē ne retāk kā reizi kalendāra gadā ir jāveic pēdējās pilnās rezerves kopijas un tai sekojošo pieauguma kopiju atjaunošanas pārbaudes.

Normatīvie akti nosaka virkni prasību nepieciešamajai dokumentācijai un iestāžu rīcībai IS darbības atjaunošanas plānošanai un atjaunošanas pārbaudēm (skatīt 8.tabulu).

Normatīvais akts[109] nosaka, ka iestādēs, kurās ir izstrādāti IS darbības atjaunošanas plāni, tie jāpārskata vismaz reizi gadā, kā arī gadījumos:

- ja izmaiņas IS var ietekmēt IS drošību;
- ja mainījušies vai ir atklāti jauni IS drošības apdraudējumi;
- ja pēkšņi pieaug IS drošības incidentu skaits vai ir noticis nozīmīgs IS drošības incidents;
- ja izmaiņas institūcijas organizatoriskajā struktūrā skar IS drošības vadības organizāciju;
- ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.

Lai pārliecinātos, vai IS darbības atjaunošanas plāns strādā un ir iespējams atjaunot informācijas sistēmu IS drošības politikā noteiktajā IS darbības atjaunošanas laikā, ir nepieciešams veikt IS darbības atjaunošanas plāna testēšanu[110].

Lai nodrošinātu IS atjaunošanu pilnā apmērā (atjaunojot ne tikai pašas IS darbību, bet arī tajā uzglabātos datus), ir jānodrošina normatīvajā aktā paredzētā IS datu rezerves kopiju veidošana un atjaunošana[111]. Lai atbildīgie darbinieki spētu kvalitatīvi nodrošināt IS darbības atjaunošanu, tiem ir jānodrošina apmācības[112].

Normatīvais akts[113] nosaka, ka visās iestādēs neatkarīgi no IS veida vai noteiktās drošības kategorijas, izstrādājot IS drošības politiku, ir jāparedz, ka iestāde nodrošina IS esošo datu rezerves kopiju veidošanu un atjaunošanu.

Gadījumos, ja iestādē tiek uzturētas paaugstinātas drošības IS, tad šādām IS ir jāizstrādā iekšējie sistēmas drošības noteikumi, kuros ir ietverta IS rezerves kopiju izgatavošanas un glabāšanas kārtība[114]. Prasību izstrādāt iekšējos sistēmas drošības noteikumus ar tajā ietvertu IS rezerves kopiju izgatavošanas un glabāšanas kārtību pamata drošības IS normatīvais akts nenosaka.

Neatkarīgi no tā, vai IS ir pamata vai paaugstinātas drošības IS, gadījumos, ja iestādes uztur integrētās valsts IS vai valsts IS savietotāju, normatīvais akts[115] nosaka prasības šo IS datu rezerves kopiju veidošanai, atjaunošanai un glabāšanai.

8.tabula

Prasības nepieciešamajai dokumentācijai un iestāžu rīcībai IS darbības atjaunošanas plānošanai un atjaunošanas pārbaudēm

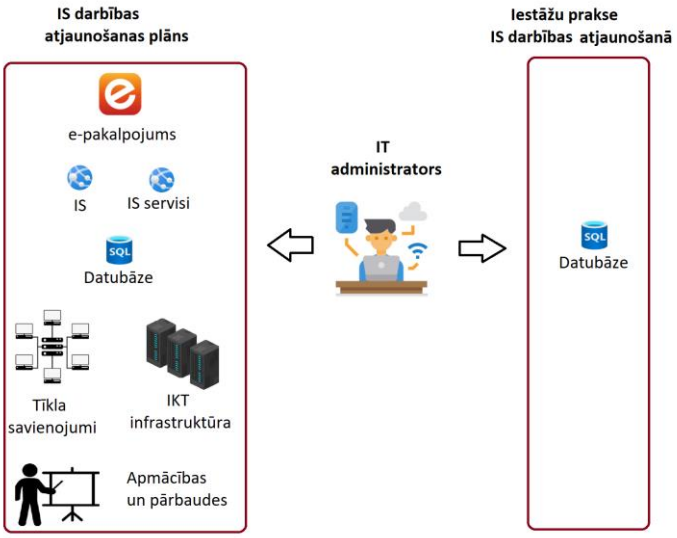
	Normatīvais akts	Iestādes IS un valsts IS		Integrētās valsts IS un savietotājs
		Pamata drošības	Paaugstinātas drošības	
IS darbības atjaunošanas plāns (dokumentācija)				
Iestādē ir izstrādāts IS darbības atjaunošanas plāns	28.07.2015. MK442 8.5.p.		X	
IS darbības atjaunošanas plāns tiek pārbaudīts (testēts) un atjaunots reizi gadā vai biežāk, ja ir bijušas būtiskas IS darbības un konfigurācijas izmaiņas vai pēc nozīmīgiem drošības incidentiem	28.07.2015. MK442 10.p.			
IS darbības atjaunošana				
Datu rezerves kopēšana, glabāšana un atjaunošana (rīcība)				
Iestāde nodrošina datu rezerves kopiju veidošanu un datu rezerves kopiju atjaunošanu	28.07.2015. MK442 15.17. p.	X	X	
Integrētajām valsts IS un savietotājam tiek veidotas rezerves kopijas (pilnās un pieauguma), un tās tiek pārbaudītas ne retāk kā reizi gadā, atjaunojot datus testa vidē	19.06.2012. MK421 10.6.p.			X
Rezerves kopiju veidošanas un atjaunošanas kārtība (dokumentācija)				
Izstrādāta IS rezerves kopiju izgatavošanas un glabāšanas kārtība	28.07.2015. MK442 25.4.p.		X	
Izstrādāta kārtība, kā pārbaudīt, vai no rezerves kopijām var atjaunot datus				
Rezerves kopiju glabāšana (rīcība)				
Pilnās rezerves kopijas tiek glabātas ģeogrāfiski nošķirtā vietā	19.06.2012. MK421 10.1.–10.5.p.			X
Rezerves kopiju glabāšanas ilgums no 1 mēneša līdz 3 gadiem				
Nedēļas, mēneša un gada kopijas tiek glabātas vietā, kurā netiek pieļauta trešo personu piekļuve un bojājumi ugunsgrēku, plūdu u.c. gadījumos				

Revīzijā konstatēts, ka no sešām iestādēm, kuras ir izstrādājušas IS darbības atjaunošanas plānus:

- trijās iestādēs ne reizi nav veiktas pārbaudes, vai IS darbības atjaunošanas plānā ietvertās procedūras IKT infrastruktūras, IS programmatūras, datu bāzu, IS servisu un e-pakalpojumu darbības atjaunošanai ir pilnīgas un pietiekamas, lai iespējami īsā laikā atjaunotu IS pieejamību.

  Lai gan visās iestādēs IS drošības politika paredz reizi gadā veikt IS darbības nepārtrauktības un atjaunošanas plāna realizācijas pārbaudi, tādas nav organizētas.

  Iestādes skaidro, ka IS darbību atjaunošanas pārbaudes tiek aizvietotas, testa vidē pārbaudot datu atjaunošanas iespējamību no rezerves kopijas. Jāatzīmē, ka datu atjaunošana no rezerves kopijas var nebūt pietiekama, ja netiek plānota un pārbaudīta pārējo IS darbībai nepieciešamo komponenšu pieejamība vai atsevišķu incidentu gadījumā atjaunojamība, piem., programmatūras atbilstošās versijas, IKT infrastruktūra, tehniskais personāls (19.attēls).



19.attēls. Vēlamā un faktiskā iestāžu prakse IS darbības atjaunošanas plāna testēšanai

- piecās iestādēs netiek nodrošinātas plānveidīgas apmācības darbiniekiem IS darbības atjaunošanā, lai gan normatīvais akts[116] paredz nodrošināt atbildīgo personu apmācības un pārbaudīt šo personu sagatavotību.

  Iestādēs atkarībā no IT struktūrvienības darbinieka specializācijas tiek organizētas apmācības par IS administrēšanas un IKT infrastruktūras uzturēšanas jautājumiem kopumā, bet neietverot IS darbības atjaunošanas simulāciju.

Vērtējot, vai iestādes nodrošina IS esošo datu rezerves kopiju veidošanu un atjaunošanu, konstatēts, ka:

- visās revīzijas apjomā iekļautajās iestādēs tiek nodrošināta datu rezerves kopiju veidošana;
- lai gan visās deviņās iestādēs tiek uzturētas paaugstinātas drošības IS, divās iestādēs nav izstrādāta datu rezerves kopiju veidošanas kārtība un kārtība datu atjaunošanai, kā tas noteikts normatīvajā aktā[117];
- lai gan integrētajām valsts IS testa vidē ne retāk kā reizi kalendāra gadā[118] ir jāveic pēdējās pilnās rezerves kopijas un tai sekojošo pieauguma kopiju atjaunošanas pārbaudes, tomēr sešās iestādēs tas netiek nodrošināts:
  - datu atjaunošanas pārbaude ir veikta tikai pēdējai pilnajai rezerves kopijai, nepārbaudot pieauguma kopijas kvalitāti un darbinieku zināšanas tās atjaunošanā, kas rada risku, ka tiks zaudēta tā daļa uzkrāto datu, kas rezervēti pieauguma kopijā;
  - iestādes paļaujas uz rezerves kopiju veidošanas sistēmā iebūvētajām automātiskajām kontrolēm, kuras rezerves kopijas izveides brīdī ziņo, vai kopija izveidota un vai tā ir izveidota bez kļūdām.
- lielākajā daļā iestāžu (septiņās iestādēs) datu rezerves gada kopijas tiek glabātas tikai vienu gadu vai vēl mazāk, nevis trīs gadus, kā tas noteikts normatīvajā aktā[119].

Iestādes šo apstākli skaidro ar to, ka datu atjaunošanai darbības nepārtrauktības nodrošināšanai svarīgi ir tieši aktuālie dati, nevis vairākus gadus uzglabātie dati.

Ieteikums

Lai gūtu pārliecību, ka valsts pārvaldē izmantotās būtiskās IS un tajās uzkrātie dati ir atjaunojami, Aizsardzības ministrijai sadarbībā ar VARAM izstrādāt pasākumu plānu, lai nodrošinātu, ka iestādēs ir izstrādāti IS darbības atjaunošanas plāni un tiek regulāri nodrošināta to pilnīguma un atbilstības pārbaude, pārliecinoties par IS pieejamības un datu atjaunošanas iespējamību noteiktajā atjaunošanas laikā.

3. Vai valsts līmenī ir noteikta nepieciešamība nodrošināt IS pieejamību un ir apzināts, kurām IS tā jānodrošina?

Vai IS pieejamība ir noteikta kā mērķis attīstības plānošanas dokumentos?

Attīstības plānošanas dokumentos[120] kopumā ir apzināts IS pieejamības nozīmīgums valstiskā līmenī, t.sk. e-pakalpojumu sniegšanai. Tomēr, izņemot vienu sasniedzamo politikas rezultātu "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam", kopumā attīstības plānošanas dokumentos nav noteikti konkrēti sasniedzamie mērķi un uzdevumi IS pieejamības nodrošināšanai un izvirzīti rezultatīvie rādītāji, pēc kuriem mērīt un novērtēt sasniegto IS pieejamību. Tādējādi attīstības plānošanas dokumentos nav identificējams rīcības ietvars IS pieejamības nodrošināšanā un valsts pārvaldē nav vienotas izpratnes par sasniedzamo IS pieejamības jomā un netiek veiktas mērķtiecīgas darbības, lai to sasniegtu.

Vienā no attīstības plānošanas dokumentiem – "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" – ir noteikts sasniedzamais rezultāts un rezultatīvais rādītājs, kas saistāms ar IKT darbības nepārtrauktības nodrošināšanu un IS pieejamību. Rādītājs paredz, ka 85% no visām paaugstinātas drošības līmeņa sistēmām un platformām ir droši rezervētas un atjaunojamas. Tomēr šī rādītāja sasniegšanai nav izvirzīti konkrēti uzdevumi un nedz VARAM (kā politikas plānošanas dokumenta sagatavotājai), nedz AiM (kā vadošajai iestādei IS drošības politikas jomā) vēl 2022.gada sākumā nebija nav skaidrs, kurš un kādā veidā nodrošinās, kā arī uzraudzīs un mērīs izvirzītā politikas rezultāta sasniegšanu.

IKT darbības nepārtrauktība, t.sk. IS un e-pakalpojumu pieejamības nepieciešamība, ir iezīmēta vairākos attīstības plānošanas dokumentos:

- "Latvijas kiberdrošības stratēģijā 2019.–2022.gadam"[121] uzsvērts, ka veiksmīgas digitālas sabiedrības priekšnoteikums ir uzticēšanās IKT risinājumu un digitālo tehnoloģiju spējai garantēt pakalpojumu pieejamību. Viens no izvirzītajiem rīcības virzieniem ir IKT izturētspēja un sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana.
- "Latvijas Nacionālajā attīstības plānā 2021.–2027.gadam"[122] norādīts, ka:
  - būtisks izaicinājums ir atrast veidu, kā nodrošināt un uzlabot publisko pakalpojumu kvalitāti, drošību un pieejamību sabiedrībai, nepieaugot publiskā finansējuma apjomam;
  - ikvienam elektroniskajam pakalpojumam un risinājumam pirms tā ieviešanas tiks veikts kiberdrošības risku izvērtējums, kā arī nodrošināta tā kiberdrošība visā tā dzīvescikla laikā, lai nodrošinātu pakalpojuma un risinājuma nepārtrauktību, integritāti un datu aizsardzību.
- "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam"[123] norādīts, ka:
  - digitālās drošības politika ietver ne tikai valsts funkciju izpildes nepārtrauktības un atjaunojamības digitālajā vidē jautājumus, bet arī digitālo drošību;
  - jāizvērtē un jāiekļauj normatīvajos aktos prasību, ka pirms jebkura IKT pakalpojuma izveides valsts iestādēm ir pienākums apzināt tā iespējamos kiberdrošības riskus, veicot kiberdrošības risku analīzi. Visā risinājuma dzīvescikla laikā ir jānodrošina kiberdrošība tā, lai nodrošinātu pakalpojuma un risinājuma nepārtrauktību, integritāti un datu aizsardzību;
  - jāizvērtē subjektu loks, kuriem ir nepieciešams izstrādāt rīcības plānu nepārtrauktas darbības nodrošināšanai. Izstrādātie rīcības plāni ir regulāri jāpārbauda, piemēram, mācību laikā, un nepieciešamības gadījumā jāpilnveido;
  - valsts pārvaldes skaitļošanas infrastruktūras koplietošanas pakalpojumu sniedzējiem jānodrošina sistēmu darbības atjaunošanas pakalpojumi, ko valsts pārvaldes institūcijas izmanto atbilstoši datu apstrādes nepārtrauktības prasību līmeņiem.

"Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" kā viens no rezultātiem kontekstā ar IKT darbības nepārtrauktības nodrošināšanu un IS pieejamību izvirzīts rādītājs – 85% no visām paaugstināta drošības līmeņa sistēmām un platformām, kas reģistrētas VIRSIS, ir droši rezervētas un atjaunojamas (atjaunojamība ir testēta). Revīzijā netika konstatēti konkrēti uzdevumi minētā rādītāja sasniegšanai, kā arī nav noteikta atbildīgā iestādē, kas veiks pārbaudes, vai paaugstināta drošības līmeņa sistēmas ir droši rezervētas un to atjaunojamība ir testēta, lai mērītu pamatnostādnēs izvirzītā rādītāja sasniegšanu.

Vēl 2022.gada sākumā gan VARAM (kā "Digitālās transformācijas pamatnostādņu 2021.–2027.gadam" sagatavotāja un atbildīgā ministrija IKT pārvaldības jomā), gan AiM (kā vadošā iestāde IT drošības politikas veidošanā un īstenošanā) informēja, ka šī rezultāta sasniegšanai vēl nav apzināts, kurš un kādā veidā mērīs šī rādītāja sasniegšanu.

Kopumā attīstības plānošanas dokumentos noteiktie mērķi un uzdevumi vairāk attiecas uz IKT infrastruktūras darbības nepārtrauktības nodrošināšanu, bet tie neiezīmē konkrētus mērķus, uzdevumus

un rezultatīvos rādītājus attiecībā uz IS pieejamības līmeni – vai un kāds IS pieejamības līmenis iestādēs ir jāsasniedz, garantējot privātpersonām pakalpojuma saņemšanu noteiktā laikā. Tādējādi attīstības plānošanas dokumentos nav identificējams rīcības ietvars IS pieejamības nodrošināšanā un valsts pārvaldē nav vienotas izpratnes par sasniedzamo IS pieejamības līmeni un netiek veiktas mērķtiecīgas darbības, lai to sasniegtu.

Ņemot vērā, ka atbildība IKT pārvaldības un IS drošības jomā ir sadrumstalota starp vairākām iestādēm, būtiski ir savlaicīgi noteikt, kurš un kādā veidā uzraudzīs kopējās tendences IS pieejamības sasniegšanā, un veikt citas nepieciešamās darbības iesaistīto iestāžu darbības koordinēšanā šī izvirzītā rādītāja sasniegšanā.

Ieteikums

Lai radītu priekšnoteikumus "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" noteiktā rezultatīvā rādītāja IS pieejamības jomā izmērīšanai, līdz pamatnostādņu īstenošanas starpposma novērtējumam[124] VARAM sadarbībā ar citām iestādēm veikt nepieciešamās darbības, lai veicinātu tā sasniegšanu.

Vai vienkopus ir apzinātas valstī izmantotās IS?

Lai gan valsts IS un IKT resursu uzskaites sistēma – VIRSIS – ir izstrādāta un ir ieviesta kopš 01.01.2020., tajā uzskaitītie dati ir nepilnīgi:

- iestādes ir reģistrējušas datus tikai par 127 no 181 valsts IS, kas bija reģistrēta iepriekš uzturētajā "Valsts informācijas sistēmu reģistrā" (turpmāk – VISR);
- tikai 19 IS pārziņi ir norādījuši, ka IS tiek izmantota iestādes pamatdarbības nodrošināšanai. Par lielāko daļu IS (123 IS) to pārziņi ir norādījuši, ka IS paredzētas iestādes iekšējo vajadzību nodrošināšanai, tātad nenodrošina datu apmaiņu ar citām sistēmām vai pakalpojumu sniegšanu, kas liek domāt, ka sistēmas nav korekti klasificētas;
- VIRSIS nav uzkrāti dati, kas varētu liecināt par IS datu apmaiņu ar citām IS un to, vai IS ir integrētā valsts IS, kas ir būtiski, lai konstatētu, vai IS ir ietekme uz citām IS.

Trūkumi informācijas uzskaitē ietekmē VARAM spēju sekmīgi plānot vienotu valsts politiku IS un to darbībai nepieciešamo IKT resursu un pakalpojumu attīstībai un uzturēšanai, kā arī nodrošināt uz pierādījumiem balstītas rīcībpolitikas iedibināšanu IKT pārvaldības jomā. Pēc revidentu domām atbilstoša un pietiekama informācija par valsts IS un ar tām saistīto IKT infrastruktūru ir priekšnoteikums vienotu IS pieejamības un IKT darbības nepārtrauktības pārvaldības principu plānošanai, noteikšanai un uzraudzībai.

Trūkumi VIRSIS uzskaitītajā informācijā neļauj identificēt tās IS, kas nodrošina pakalpojumu sniegšanu privātpersonām un datu apmaiņu ar citām IS, un attiecīgi tieši šīm IS un to darbību atbalstošajai IKT infrastruktūrai būtu jāsasniedz atbilstoša līmeņa pieejamība un jāplāno resursi tās nodrošināšanai.

Jau 2019.gadā[125] Valsts kontroles revīzijā tika secināts, ka valstī gandrīz desmit gadu laikā tā arī nav izdevies atrisināt IKT resursu uzskaites un šo datu apkopošanas problēmas uz pierādījumiem balstītas rīcībpolitikas iedibināšanai IKT pārvaldības jomā. Iepriekš izveidotais valsts IS reģistrs bija novecojis un nenodrošināja visas VARAM nepieciešamās informācijas uzskaiti.

Kopš 01.01.2020. VARAM ir izveidojis jaunu sistēmu – VIRSIS, kurā nodrošināt valsts informācijas sistēmām un to darbībai nepieciešamo informācijas un komunikācijas tehnoloģiju resursu un pakalpojumu uzskaiti[126]. Saskaņā ar normatīvo aktu[127] VARAM to izmanto, lai valsts IKT pārvaldības funkciju izpildei nodrošinātu:

- vienotu valsts politiku valsts IS un to darbībai nepieciešamo IKT resursu un pakalpojumu uzskaites, attīstības un uzturēšanas jomā;
- centralizētu elektronisko vidi strukturētas informācijas iegūšanai par valsts IS un to darbības uzturēšanai un attīstībai nepieciešamajiem IKT resursiem un pakalpojumiem.

VIRSIS ir nozīmīgs informācijas uzskaites reģistrs VARAM funkciju[128] izpildei ar mērķi:

- apkopot un uzturēt datus par elektronisko pārvaldi un valsts IKT, tajā skaitā elektroniskajiem pakalpojumiem, valsts IKT infrastruktūru un IS (arī valsts IS), kā arī iestādēm nepieciešamā IKT atbalsta tehniskajiem un finanšu resursiem un cilvēkresursiem;
- nodrošināt informācijas sabiedrības, elektroniskās pārvaldes un valsts IKT attīstības atbalsta pasākumu ierosināšanu, plānošanu, vērtēšanu, ieviešanu, vadību, koordināciju, uzraudzību un kontroli;
- nodrošināt informācijas sabiedrības, elektroniskās pārvaldes un valsts IKT pārvaldības politikas īstenošanai nepieciešamās valsts un pašvaldību institūciju, kā arī nevalstisko organizāciju darbības koordināciju un to savstarpējās sadarbības organizēšanu starpnozaru (pārresoru) līmenī.

Lai gan IS pieejamība kā VIRSIS izveides mērķis nav identificēta, tomēr revidentu ieskatā IS pieejamības plānošanai, resursu novirzīšanai tās nodrošināšanai un uzraudzībai viens no priekšnoteikumiem ir informācijas pieejamība par valsts pārvaldē izveidotajām un izmantotajām informācijas sistēmām. Tas ļautu vienuviet identificēt valstī būtiskākās IS, kuras ir svarīgas valsts kopējās IKT arhitektūras kontekstā.

No normatīvā akta[129] izriet, ka līdz 08.08.2020. valsts IS pārziņiem bija jānodrošina datu ievade VIRSIS par to pārziņā esošajām valsts IS un to darbībai nepieciešamo IKT resursu un pakalpojumu. Līdz tam izmantotās sistēmas VISR darbība tika pārtraukta.

Revīzijā konstatēts, ka kopš sistēmas ieviešanas VARAM vēl nav veikusi VIRSIS uzskaitīto datu par valsts IS un IKT resursiem izvērtējumu un analizējusi uzrādīto datu pilnīgumu un atbilstību, tostarp,

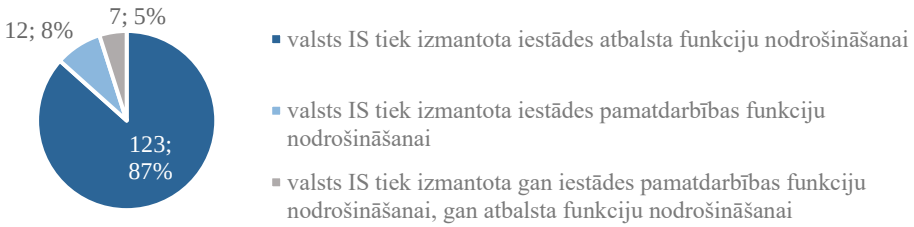
apzinot, vai iepriekš VISR uzskaitītās valsts informācijas sistēmas ir reģistrētas jaunajā sistēmā VIRSIS.

Analizējot VIRSIS uzskaitītos datus, kas ir pieejami atvērto datu portālā[130], konstatēti vairāki būtiski faktori, kas liecina, ka VIRSIS uzskaitītā informācija ir nepilnīga vai neatbilstoši uzrādīta un VARAM kā VIRSIS pārzinei tā būtu detalizēti jāvērtē, tādējādi uzlabojot datu kvalitāti VIRSIS:

- ne visi pārziņi un ne visas valsts IS ir reģistrējuši jaunajā VIRSIS sistēmā. Lai gan laika gaitā var tikt likvidētas gan valsts IS, gan to pārziņi, tomēr revīzijā konstatētās atšķirības ir būtiskas un nepieciešams veikt detalizētu to izvērtējumu.

  VIRSIS informāciju ir snieguši 55 IS pārziņi, uzrādot informāciju par 284 IS un tajās uzturētiem reģistriem. Veicot iepriekš izmantotā VISR un VIRSIS datu salīdzināšanu, konstatēts, ka:

  - iepriekš izmantotajā VISR datus bija snieguši 83 IS pārziņi, līdz ar to ne visi pārziņi datus ir reģistrējuši arī jaunajā sistēmā. Piemēram, Valsts kase un Valsts zemes dienests nav reģistrējuši nevienu IS;
  - VIRSIS sniedz datus tikai par 127 no 181 IS, kas iepriekš bija reģistrētas VISR. Piemēram, deviņās revīzijas izlasē iekļautajās iestādēs tika konstatētas 38 valsts IS, bet VIRSIS sistēmā informācija bija ievadīta tikai par 32.
- tikai 12 gadījumos IS pārziņi ir norādījuši, ka IS tiek izmantota iestādes pamatdarbības nodrošināšanai, kas saskaņā ar aprakstu[131] nozīmē, ka sistēma tiek izmantota, lai veidotu un nodrošinātu iestādes "ārējos" pakalpojumus, bet septiņām IS – gan pamatdarbības, gan atbalsta nodrošināšanai. Būtiski lielākā daļa IS (123 IS) ir paredzētas iestādes iekšējo vajadzību nodrošināšanai (20.attēls).



20.attēls. VIRSIS reģistrēto valsts IS izmantošanas veids

Revidentu ieskatā IS pārziņi ne vienmēr ir norādījuši pareizu IS izmantošanas veidu. Kā atbalsta sistēma ir norādīta IS, kas tiek izmantota iestādes pamatdarbības nodrošināšanai un pakalpojumu sniegšanai privātpersonām un tādējādi vistiešākajā veidā atbilst kategorijas "IS pamatdarbības funkcijas nodrošināšanai" aprakstam. Piemēram, kā atbalsta sistēmas, kas saskaņā ar aprakstu nodrošina iestāžu "iekšējās" vajadzības, VIRSIS ir reģistrētas:

- VAS "Latvijas Valsts radio un televīzijas centrs" uzturētā "eParaksts informācijas sistēma", kura tiek plaši izmantota valsts pārvaldē, nodrošinot eID kartēm sertifikātu izsniegšanu, laika zīmogu izsniegšanu un fizisko personu elektroniskās identitātes apliecināšanu;
- visas Valsts ieņēmuma dienesta IS, kas tiek izmantotas nodokļu administrēšanas jomā;

- Lauku atbalsta dienesta uzturētā "Lauku atbalsta dienesta informācijas sistēma", kas tiek izmantota lauksaimniekiem paredzēto atbalsta pasākumu administrēšanai;
- visas Pilsonības un migrācijas lietu pārvaldes IS (Personu apliecinošu dokumentu IS, Uzturēšanās atļauju IS u.c.), kas ir nozīmīgs informācijas avots ne tikai Pilsonības un migrācijas lietu pārvaldes funkciju nodrošināšanai, bet arī citām iestādēm. Tāpat arī Uzņēmumu reģistra IS reģistrēta kā atbalsta IS;
- visas Valsts reģionālās attīstības aģentūras IS (Elektronisko iepirkumu sistēma, e-Adreses sistēma u.c.), kas ir nozīmīgi risinājumi valsts pārvaldes darbības nodrošināšanā.

- VIRSIS nav uzkrāti dati par IS datu apmaiņu ar citām IS un to, vai IS ir integrētā valsts IS, kas ir būtiski, lai konstatētu, vai IS ietekmē citas IS.

  Lai gan saskaņā ar normatīvo aktu[132] un arī VIRSIS aprakstu[133] sistēmā ir datu lauks, lai norādītu API/Tīmekļa pakalpes, šobrīd šādas informācijas ievietošana nav obligāta. Vienlaikus revidenti konstatēja, ka iepriekš izmantotajā VISR 121 IS bija norādīts, ka tās nodrošina datu apmaiņu, no tām 74 ir reģistrētas jaunajā VIRSIS sistēmā, bet vairs nenorādot pazīmi par datu apmaiņu vai integrāciju;

- turklāt revīzijā konstatēts, ka VIRSIS nav uzkrāta informācija par visām IS, kurās tiek uzkrāti būtiski dati un kuras ir būtiskas pakalpojumu sniegšanā privātpersonām, jo saskaņā ar normatīvajā aktā noteikto[134] VIRSIS ir jāiekļauj dati tikai par valsts IS. Piemēram, revidenti identificēja, ka VIRSIS nav pieejami dati:
  - par astoņām IS, kas ir identificētas Valsts civilās aizsardzības plānā[135]. No tām trijās VSIA "Latvijas Vides, ģeoloģijas un meteoroloģijas centrs" (reģ.nr. 50103237791) uzturētajās IS – Meteoroloģisko prognožu sistēma, Hidroloģisko prognožu sistēma un Jūras datu portāls – dati tiek atjaunoti 24/7 režīmā;
  - par pašvaldībās izmantotajām IS, kurās tiek nodrošināta pašvaldību funkciju veikšana, tostarp pakalpojumu sniegšana iedzīvotājiem.

  Revidentu ieskatā, nepaplašinot normatīvajā aktā paredzēto VIRSIS tvērumu saistībā ar valstī izmantoto IS un saistīto IKT resursu uzskaiti, valstī nebūs iespējams centralizētā veidā iegūt informāciju par visām privātpersonām un savstarpējā iestāžu datu apmaiņā būtiskām IS.

Ieteikumi

Lai nodrošinātu to, ka VIRSIS uzskaitītie dati ir izmantojami VARAM funkciju īstenošanā un sniedz skaidru priekšstatu par valsts IKT resursiem un IS, VARAM:

- *pārliecināties, ka VIRSIS sistēmā ir reģistrēti visi IS pārziņi un ir uzskaitītas visas būtiskās IS;*
- *veikt VIRSIS sistēmā uzskaitīto datu kvalitātes pārbaudi, pārliecinoties par datu pilnīgumu, informācijas satura atbilstību VIRSIS uzskaites nosacījumiem un būtībai.*

VARAM viedoklis

Par veikto revīziju

VARAM atzīst, ka revīzijas tēma šobrīd ir īpaši aktuāla un tās ietvaros konstatētie fakti atklāj konkrētus trūkumus valsts pakalpojumu un IKT pārvaldības politiku ieviešanā un atsevišķās jomās arī pašreizējai situācijai atbilstoša politikas plānojuma un tiesiskā regulējuma neesamību. VARAM šobrīd intensīvi strādā gan pie valsts pakalpojumu politikas plānošanas dokumentu, gan IKT pārvaldības tiesiskā regulējuma, gan IKT nodrošinājuma un tā pārvaldības procesu un tehnoloģisko risinājumu attīstības.

VARAM piedāvā turpmākās darbības veikt balstoties uz jau uzsāktām politikas plānošanas un tiesiskā regulējuma izstrādes darbībām, kā arī attiecīgo reformu ieviešanai jau ieplānoto Atveseļošanās un noturības mehānisma un jaunā plānošanas perioda Eiropas Savienības struktūrfondu finansējumu, piedāvā turpmāko rīcību, kas atsevišķos punktos atšķiras no revīzijas ziņojuma ieteikumos formulētā.

Konkrēti – VARAM, atzīstot revīzijā konstatētās atsevišķās pretrunas pieejamības prasībās, uzskata, ka pieejamības prasību regulējums ir novecojis un varētu būt pelnījis vēl asāku kritiku. Valsts pakalpojumu pārvaldības reforma, ko VARAM ir uzsācis, izstrādājot un gatavojot saskaņošanai ar ministrijām valsts pakalpojumu pārvaldības koncepciju, cita starpā paredzēs precīzu un pamatotu pieejamības prasību izvirzīšanu konkrētiem valsts pakalpojumiem. Katram no valsts pakalpojumiem tiks definēti piegādes kanāli, kas vairumā gadījumu ietvers arī e-pakalpojumu, jeb elektroniskas pašapkalpošanās kanālu. VARAM uzskata, ka prasības elektroniskās pašapkalpošanās funkcionalitātes pieejamībai ir nosakāmas un to izpildes vai neizpildes ietekmes ir vērtējamas konkrēto valsts pakalpojumu un to pieejamības prasību kontekstā.

No otras puses – valsts pārvaldes IKT risinājumu arhitektūra tiek mērķtiecīgi attīstīta tā, lai samazinātu īpaši augstas ietekmes IKT resursu un pakalpojumu skaitu, vienlaicīgi ar to nodrošinātu šiem īpaši augstas ietekmes resursiem un pakalpojumiem īpaši augstus pieejamības līmeņus. Piemēram, Valsts informācijas sistēmu savietotāja VISS jaunās paaudzes risinājums datu agregātors (turpmāk - DAGR), kas nodrošinās arī datu īslaicīgas alternatīvas uzkrāšanas, jeb t.s. "kešošanas" funkcionalitāti, pēc tā pilnvērtīgas ieviešanas būtiski samazinās valsts pakalpojumu (t.sk. datu pakalpojumu) pieejamības atkarību no datu primāro avotu – valsts reģistru tehnisko risinājumu pieejamības. Tādējādi, reģistriem, kas savu datu kontrolētu izplatīšanu uzticēs DAGR risinājumam, reģistru primāro datu bāzu pieejamības prasības varēs samazināt, uzturot tās pietiekami augstā līmenī tikai reģistru iestāžu darba un plānoto datu apstrādes un apmaiņu procesu laikā. Īpaši augstas pieejamības prasības tiks izvirzītas arī portālam Latvija.lv un ar to saistītajām koplietošanas komponentēm, kuru faktiskā pieejamība tiek stingri uzraudzīta jau šobrīd.

VARAM uzskata, ka ierobežotu resursu apstākļos rīcībai dažāda veida valsts IKT risinājumu pieejamības nodrošināšanā un uzraudzībā ir jābūt atšķirīgai un fokusētai uz attiecīgā veida resursam pamatoti izvirzāmām pieejamības prasībām. Savietotājiem un koplietošanas komponentēm prioritāra ir darbības nepārtrauktība, bet reģistriem – to datu aizsardzība un darbības atjaunošanas spējas. Vispārēja pieejamības rādītāju mērīšana, neapšaubāmi ir jāpanāk, tomēr VARAM piedāvātā tās īstenošanu pakārtot valsts pārvaldes IKT infrastruktūras attīstības projektu plāniem.

Par revīzijas secinājumiem

VARAM kopumā piekrīt secinājumiem kas ir izdarīti par sistēmas VIRSIS ieviešanas pašreizējo stāvokli. VIRSIS datu kvalitātes un nepilnības problēmu, uz kurām ir korektas norādes ziņojumā, cēloņi ir saistīti gan ar VIRSIS esošās versijas funkcionāliem ierobežojumiem, gan sistēmu pārziņu pietiekamu ieinteresētību un iesaisti. VARAM šobrīd strādā abos virzienos, gan attīstot VIRSIS funkcionalitāti, izmantojot tam vecā plānošanas perioda struktūrfondu finansējumu, gan veicot datu kvalitātes uzlabošanas aktivitātes, kas šogad ir iekļautas VARAM ministrijas prioritāro darbu plānā.

Kā apliecina arī Digitālās transformācijas pamatnostādnēs formulētais mērķis, VARAM uzskata pārbaudītus (testētus reāli īstenojot) sistēmu darbības atjaunošanas plānus par svarīgu un pārskatāmā nākotnē sasniedzamu mērķi, kura reālu sasniegšanu un izpildes uzraudzību veicinās MK šogad pieņemtie lēmumi par valsts pārvaldes kiberdrošības spēju nostiprināšanu. Uzskatām, ka darbības šajā jomā ir jāplāno un jāīsteno Aizsardzības ministrijas un VARAM sadarbībā, t.i. no revīzijas ziņojuma ieteikumu viedokļa.

Par revīzijas ieteikumiem un to ieviešanu

Revīzijas ieteikumi ir saprotami un VARAM apņemas veikt revīzijas ieteikumu ieviešanas termiņu tabulā norādītās darbības norādītajos termiņos.

Aizsardzības ministrijas viedoklis

Par veikto revīziju

Ņemot vērā ģeopolitisko situāciju, arvien lielāka uzmanība tiek pievērsta arī drošībai Latvijas kibertelpā. Dažāda veida Informācijas tehnoloģiju drošības incidenti var ietekmēt valsts informācijas sistēmu un e-pakalpojumu pieejamību. Aizsardzības ministrija apzinās, ka kiberdrošība ir svarīgs, lai arī nebūt ne vienīgais, elements normatīvajos aktos noteiktās informācijas sistēmu un e-pakalpojumu pieejamības nodrošināšanā. Ņemot vērā arvien pieaugošās digitalizācijas tendences un e-pakalpojumu tvēruma paplašināšanos, uzskatām, ka Valsts kontroles revīzija kopumā ir bijusi nepieciešama un tā ir veikta īstajā laikā. Vienlaikus ir jāuzsver, ka tieši kiberdrošības jomā attīstība notiek nepārtraukti un pie vairāku trūkumu, uz kuriem ir norādīts arī Valsts kontroles ziņojumā, novēršanas darbs ir uzsākts un notika jau revīzijas veikšanas laikā.

Par revīzijas secinājumiem

Aizsardzības ministrija kopumā piekrīt Valsts kontroles secinājumiem un apzinās problēmas un izaicinājumus esošajā kiberdrošības pārvaldības modelī. Aizsardzības ministrija, identificējot nepietiekamo valsts pārvaldes iestāžu kiberdrošības līmeni un trūkumus kiberdrošības pārvaldības modelī, iesniedza Ministru Kabinetā informatīvo ziņojumu "Par valsts kiberdrošības pārvaldības uzlabošanu". Ministru kabinets šo ziņojumu izskatīja 2022. gada 7. jūnijā, atbalstot Nacionālā kiberdrošības centra izveidi no 2023. gada 1. janvāra. Ziņojumā tostarp ir ietverti praktiski priekšlikumi valsts un pašvaldību iestāžu IT resursu drošības uzlabošanai, kā arī šo iestāžu uzraudzībai sistemātiskā un strukturētā veidā. Iestāžu uzraudzībai, ņemot vērā ziņojumā sniegtos priekšlikumus, būtu jābalstās uz regulāriem iestāžu IT sistēmu auditiem, ciešāku uzraudzību no jaunveidojamā Nacionālā kiberdrošības centra puses, kā arī CERT.LV drošības operāciju centru izvietošanu datu koplietošanas centros.

Nacionālā kiberdrošības centra izveides mērķis ir kiberdrošības pārvaldības uzlabošana, risinot tādus izaicinājumus kā atšķirīgs kiberdrošības līmenis valsts un pašvaldību iestādēs, kvalificēta personāla un konkurētspējīga atalgojuma nodrošināšana, kā arī Eiropas Savienības tiesību aktos noteikto funkciju veikšana kiberdrošības jomā. Centra uzdevumi būs Latvijas kiberdrošības stratēģijas izstrāde, nacionālās kiberdrošības politikas koordinācija un tās ieviešanas uzraudzība, valsts informācijas sistēmu attīstības projektu drošības prasību izvērtēšana, Eiropas Savienības tiesību aktos noteikto kiberdrošības prasību izpilde, tostarp valsts funkcionēšanai būtisko un svarīgo vienību identificēšana un uzraudzība, kā arī kiberdrošības incidentu risināšana un arī valsts pārvaldes un plašākas sabiedrības informēšana par kiberdrošību.

Saistībā ar Nacionālā kiberdrošības centra izveidi un citiem Aizsardzības ministrijas sagatavotajā informatīvajā ziņojumā identificētajiem risinājumiem kiberdrošības uzlabošanai valstī, tuvākajā laikā apstiprināšanai tiks virzīti vairāki būtiski grozījumi normatīvajos aktos, tai skaitā Informācijas tehnoloģiju drošības likumā, kā arī vairākos Ministru kabineta noteikumos un citos normatīvajos aktos.

Līdz ar to Aizsardzības ministrija uzskata, ka tai ir skaidrs redzējums, kurš un kādā veidā nodrošinās Digitālās transformācijas pamatnostādnēs ietverto sasniedzamo rezultātu, kas saistāms ar IKT darbības

nepārtrauktības nodrošināšanu un IS pieejamību, sasniegšanu un, kā uzraudzīs un mērīs izvirzītā politikas rezultāta sasniegšanu. Ir jāuzsver, ka Digitālās transformācijas pamatnostādnes tika apstiprinātas 2021. gada 7. jūlijā, savukārt jaunā Latvijas kiberdrošības stratēģija tiks izstrādāta līdz 2022. gada beigām. Līdz ar to Aizsardzības ministrijai nav bijusi iespēja šo sasniedzamo mērķi iekļaut stratēģiskās plānošanas dokumentos un Aizsardzības ministrija uzskata, ka tā ir spērusi pirmos soļus, lai virzītos uz Digitālās transformācijas pamatnostādnēs ietverto sasniedzamo uzdevumu izpildi. Vienlaikus arī apzināmies, ka šie ir tikai pirmie soļi un noteikto sasniedzamo uzdevumu izpildei ir vajadzīga ne tikai stratēģiskās plānošanas dokumentu un normatīvo aktu papildināšana, bet arī praktiska valsts un pašvaldības iestāžu uzraudzības pilnveidošana, kas būs iespējama, atvēlot šiem mērķim atbilstošus finanšu un personāla resursus Nacionālajā kiberdrošības centrā.

Vienlaikus Aizsardzības ministrija vēlas uzsvērt, ka kopumā IT drošības incidenti ir tikai viena daļa no iemesliem, kādēļ informācijas sistēmas un e-pakalpojumu var nebūt pieejami. Piemēram, informācijas sistēmas darbības pārtraukumi var rasties arī sistēmas uzturēšanas darbu rezultātā vai tās pārslodzes, vai arī kļūdainas konfigurācijas dēļ, kas nav viennozīmīgi klasificējams kā kaitīgs notikums vai nodarījums. Līdz ar to ir jānorāda, ka revīzijas tvērums apskata tikai nelielu daļu no Aizsardzības ministrijas un CERT.LV kompetences kiberdrošības jomā, un kopumā uzdevumi, kas saistīti ar valsts kiberdrošības stiprināšanu, ir daudz plašāki. Savukārt lielākā daļa no sistēmu pieejamības jautājumiem būtu jārisina ar monitorēšanas risinājumiem datu centru un iestāžu līmenī.

Par revīzijas ieteikumiem un to ieviešanu

Kopumā Aizsardzības ministrija neiebilst Valsts kontroles ieteikumiem un uzskata, ka tie ir praktiski realizējami noteiktajos termiņos. Kā jau minēts, saistībā ar Nacionālā kiberdrošības centra izveidi un centieniem stiprināt valsts kiberdrošības pārvaldību, Aizsardzības ministrija jau ir uzsākusi darbu pie vairāku normatīvo aktu izstrādes, tai skaitā, pie grozījumu izstrādes Informācijas tehnoloģiju drošības likumā, kā arī ar to saistītajos Ministru kabineta noteikumos. Tāpat ir jānorāda, ka Aizsardzības ministrija līdz 2022. gada beigām Ministru kabinetā plāno iesniegt apstiprināšanai Latvijas Kiberdrošības stratēģiju 2023.-2026. gadam.

Līdz ar Kiberdrošības stratēģijas, kā arī vairāku normatīvo aktu izstrādi, Aizsardzības ministrija ieviesīs Valsts kontroles ieteikumus, veidojot efektīvāku un skaidrāku valsts kiberdrošības pārvaldību, tai skaitā, ieviešot sistemātisku un strukturētu Informācijas tehnoloģiju likuma un Ministru Kabineta noteikumu Nr. 442 subjektu uzraudzību, kā arī definējot skaidrus virzienus un uzdevumus nacionālās kiberdrošības stiprināšanai jaunajā Kiberdrošības stratēģijā.

Vienlaikus ir jāapzinās, ka, lai ieviestu Valsts kontroles ieteikumus, ir nepieciešams ne tikai izstrādāt pasākumu plānu, bet uzraugošajām iestādēm ir jābūt atbilstošiem rīkiem, lai spētu efektīvi īstenot identificēto uzdevumu izpildes kontroli un noteikt atbilstošas sankcijas, t.sk., galējā gadījumā arī naudas sodu veidā.

Aizsardzības ministrija apliecina, ka izprot Valsts kontroles revīzijā izteiktos secinājumus un ieteikumus, kā arī apņemas savas kompetences ietvaros veikt nepieciešamos pasākumus, lai uzlabotu valsts informācijas sistēmu un e-pakalpojumu pieejamību.

Revīzijas raksturojums, kritēriji un metodes

Revīzijas mērķis

Revīzijas mērķis ir pārliecināties, ka valstī:

- spēkā esošais normatīvais regulējums rada priekšnoteikumus, lai nodrošinātu IS un e-pakalpojumiem noteiktā pieejamības līmeņa sasniegšanu;
- var paļauties uz iedzīvotāju pieprasītāko e-pakalpojumu sniegšanai izmantoto IS pieejamību un e-pakalpojumu saņemšanu.

Revīzijas pieeja

Revīzijas pieeja veidota, fokusējoties uz vienu no trim normatīvajā aktā[136] ietvertajām prasībām IS drošības īstenošanai, t.i., lai nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikā pēc informācijas pieprasīšanas). Līdz ar to revīzijā kopumā tika vērtēts, vai iestādēs pēc vienotiem principiem tiek nodrošināta svarīgāko IS pieejamība un ar to saistītās IKT infrastruktūras darbības nepārtrauktība.

Kopumā revīzijā netiek apšaubīta IS pieejamības un IKT darbības nepārtrauktības nodrošināšana iestādēs, bet, ņemot vērā, ka riski var iestāties jebkurā brīdī un iestādēm ir jāveic priekšdarbi, lai to iestāšanos un ietekmi samazinātu, revīzijā tika gūta pārliecība, ka iestādēs tiek veiktas nepieciešamās preventīvās darbības, lai nodrošinātu nepieciešamo IS pieejamības līmeni, kā arī iestādes ir gatavas incidentu gadījumā atjaunot IS darbību līdz stāvoklim, kāds tas bija pirms incidenta.

Revīzijas pieejas jautājumi grupēti piecās galvenajās sadaļās:
- IS pieejamības nepieciešamības apzināšana valstiskā līmenī;
- IS apzināšana vienkopus valstiskā līmenī, lai noteiktu būtiskākās IS, kurām jānodrošina augstākie pieejamības rādītāji;
- normatīvajos aktos noteiktās prasības IS pieejamībai;
- iestādēs realizētā IS un e-pakalpojumu pieejamība, IKT darbības nepārtrauktība un gatavība nodrošināt IS atjaunošanu incidentu gadījumos;
- valsts līmenī veiktais IS pieejamības līmeņa un IS nepieejamības seku izvērtējums.

Revīzijas pārbaudes jautājumos, kuros nacionālās prasības IS pieejamībai un IKT darbības nepārtrauktībai bija vispārīgas, tika izmantoti labās prakses piemēri (COBIT4.1., ITIL u.c.) Labās prakses standarti IT jomā tiks izmantoti, arī lai identificētu tās IS pieejamības un IKT darbības nepārtrauktības jomas, kuras nav pietiekoši identificētas un aprakstītas nacionālajās prasībās.

Juridiskais pamatojums

Lietderības revīzija "Vai varam paļauties uz informācijas sistēmu pieejamību un e-pakalpojumu saņemšanu?" ir veikta, pamatojoties uz Valsts kontroles Revīzijas un metodoloģijas departamenta 2020.gada 9.septembra revīzijas uzdevumu Nr.2.4.1-38/2020.

Revīziju veica revīzijas grupas vadītājs – informācijas sistēmu auditors Valdis Kaļupnieks, informācijas sistēmu auditors Rolands Avišāns, informācijas sistēmu auditors Mārtiņš Vilmanis (no 26.04.2021.) un informācijas sistēmu auditore Līga Nagle (līdz 23.04.2021.).

Revidentu un revidējamās vienības atbildība

Valsts kontroles revidenti ir atbildīgi par revīzijas ziņojuma sniegšanu, kas pamatojas uz revīzijas laikā gūtiem atbilstošiem, pietiekamiem un ticamiem revīzijas pierādījumiem.

VARAM, AiM un revīzijas izlases apjomā iekļautās iestādes ir atbildīgas par normatīvo aktu ievērošanu un revidentiem sniegtās informācijas patiesumu.

Revīzijas apjoms un ierobežojumi

Revīzija ir veikta saskaņā ar Latvijas Republikā atzītiem starptautiskajiem revīzijas standartiem. Revīzija plānota un veikta tā, lai iegūtu pietiekamu pārliecību, ka iestādēs tiek sasniegts noteikts IS un e-pakalpojumu pieejamības līmenis, tai skaitā ir radīti priekšnoteikumi IKT darbības nepārtrauktības, IS un e-pakalpojumu pieejamības nodrošināšanai.

Revīzija veikta par 2019.–2021.gadu, tomēr IS un e-pakalpojumu pieejamības novērtēšanai izmantoti dati arī no citiem periodiem.

Revīzijas ziņojuma apjomā:

- lai novērtētu attīstības plānošanas dokumentos izvirzītās prasības IS pieejamības jomā, iekļautas VARAM un AiM;
- lai novērtētu iestādēs sasniegtā IS un e-pakalpojumu pieejamības līmeni, kā arī ieviestos priekšnoteikumus IKT darbības nepārtrauktības un sasniedzamā IS un e-pakalpojumu pieejamības līmeņa nodrošināšanai, ir iekļautas deviņas iestādes:
  - [IP];
  - [IP];
  - [IP].
- lai novērtētu valsts līmenī uzkrāto informāciju par IKT incidentiem un to ietekmi uz valstiskā līmenī sasniegto IS pieejamību, iekļauta CERT.LV;

- lai identificētu starptautiskajā līmenī noteiktās prasības IS pieejamībai tādām nacionālā līmeņa IS, kurās informācijas apmaiņa notiek ar citām valstīm, iekļauta informācija no revidentu veiktās 13 ministriju (informāciju apkopojot visa resora ietvaros) un 15 citu neatkarīgo iestāžu aptaujas.

Revīzijas ierobežojumi:

Revīzijā tika vērtēta tehnisko resursu pieejamības pārvaldība, lai nodrošinātu IS darbību un e-pakalpojumu saņemšanu, bet netika vērtēta:

- iestāžu funkciju izpildes darbības nepārtrauktības nodrošināšana;
- atbilstība specifiskajām prasībām, kas izvirzītas valsts kritiskajai infrastruktūrai un kritiskajā infrastruktūrā iekļautajām IS;
- valsts pārvaldē piedāvāto e-pakalpojumu pilnīgums, saturs un funkcionalitāte (to starp, pieejamība personām ar īpašām vajadzībām).

Vērtēšanas kritēriji

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
1. Vai IS pieejamība ir valsts līmenī apzināta un ir izvirzīts mērķis un konkrēti uzdevumi tās nodrošināšanai?		
	Attīstības plānošanas dokumentos ir izvirzīti mērķi IS un ar to saistītās IKT infrastruktūras pieejamībai.	⊗ **Kritēriji nav sasniegti** Attīstības plānošanas dokumentos ir apzināts IS pieejamības nozīmīgums, tomēr tajos nav izvirzīti konkrēti sasniedzamie mērķi, uzdevumi un izmērāmi rezultatīvie rādītāji, izņemot "Digitālās transformācijas pamatnostādnēs 2021.–2027.gadam" ietverto rādītāju – 85% paaugstināta drošības līmeņa IS ir droši rezervētas un atjaunojamas. Tomēr nedz VARAM (kā atbildīgā iestāde IKT pārvaldības jomā), nedz AiM (kā vadošā iestāde IT jomā) vēl 2022.gada sākumā nebija izvirzījusi uzdevumus, lai nodrošinātu izvirzītā rādītāja izpildi. Neviena no tām neuzrauga, vai e-pakalpojumu un tos atbalstošo IS pieejamība tiek sasniegta.
	Attīstības plānošanas dokumentos ir definēti uzdevumi, izmērāmi rezultatīvie rādītāji, atbildīgās iestādes un tiek plānots nepieciešamais finansējums IKT darbības nepārtrauktības un IS pieejamības nodrošināšanai.	

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
2. Vai valsts rīcībā vienkopus ir pieejama informācija, lai plānotu IS pieejamību un ar to saistītās IKT infrastruktūras pārvaldību?		
2.1. Vai valstī vienkopus ir apzinātas un uzskaitītas izmantotās IS un iestāžu funkcijas, ko tās atbalsta?	Vienkopus ir pieejama informācija par valsts pārvaldes iestādēs izmantotajām IS un iestāžu funkcijām, kuru izpildē tiek izmantotas konkrētās IS.	**Kritērijs sasniegts daļēji** Lai gan VIRSIS ir ieviests kopš 01.01.2020., tajā uzskaitītie dati ir nepilnīgi: - iestādes ir reģistrējušas datus tikai par 127 no 181 valsts IS, kas bija reģistrēta iepriekš VIRS reģistrā; - VIRSIS nav uzkrāti dati par IS datu apmaiņu ar citām IS un to, vai IS ir integrētā valsts IS, kas ir būtiski, lai konstatētu, vai IS ietekmē citas IS.
	Apzinātas valstī būtiskākās IS.	**Kritērijs nav sasniegts** VARAM rīcībā nav kvalitatīvas informācijas par visām IS, kas ir priekšnoteikums vienotu IS pieejamības un IKT darbības nepārtrauktības pārvaldības principu plānošanai, noteikšanai un uzraudzībai. VARAM nav veikusi VIRSIS uzskaitīto IS izvērtējumu (analīzi), kas ļautu identificēt valstī būtiskākās IS, kuras ir svarīgas valsts kopējās IKT arhitektūras kontekstā.
2.2. Vai izmantotās IS tiek izvērtētas pēc vienotiem principiem, lai diferencētu prasības sasniedzamajam pieejamības līmenim, atkarībā no IS svarīguma iestādes darbības nodrošināšanā?	Apzinātās IS valstī tiek izvērtētas pēc vienotiem principiem, lai diferencētu prasības sasniedzamajam pieejamības līmenim.	**Kritērijs nav sasniegts** Tikai 19 IS pārziņi ir norādījuši, ka IS tiek izmantota iestādes pamatdarbības nodrošināšanai. Par lielāko daļu IS (123 IS) to pārziņi ir norādījuši, ka IS paredzētas iestādes iekšējo vajadzību nodrošināšanai, tātad nenodrošina datu apmaiņu ar citām sistēmām vai pakalpojumu sniegšanu, kas liek domāt, ka sistēmas nav korekti klasificētas.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
3. Vai normatīvajos aktos ir noteiktas prasības, kas iestādēm ir jāievieš IS pieejamības nodrošināšanai?		
3.1. Vai normatīvajos aktos ir noteikts IS pieejamības līmenis, kas iestādei ir jāsasniedz?	Normatīvajos aktos ir noteikti IS darbības nepārtrauktības un pieejamības radītāji, kas iestādēm ir jāsasniedz.	**Kritērijs sasniegts daļēji** Saskaņā ar normatīvo aktu[137] integrētajām valsts IS ir jānodrošina IS pieejamības līmenis 98%, savietotājam – 99%, bet atsevišķām integrētajām valsts IS specifiskajos normatīvajos aktos pieejamības līmeņi ir noteikti zemāki. Pārējām iestādēs izmantotajām IS sasniedzamā IS pieejamības līmeņa noteikšana pamatā tiek atstāta iestādes ziņā.
3.2. Vai normatīvie akti diferencē prasības IS atkarībā no IS būtiskuma?	Normatīvie akti diferencē IS pēc būtiskuma grupām.	**Kritērijs ir sasniegts** Normatīvais akts[138] nosaka, ka nacionālā līmenī IS valstī iedala divās kategorijās – pamata un paaugstinātas drošības sistēmas.
	Iestādes IS izvērtējums: - Iestāde ir veikusi IS izvērtēšanu atbilstoši MK442 noteiktajiem kritērijiem, iedalot IS pamata vai paaugstinātas drošības sistēmās (MK442 7.p.); - Ja iestāde uztur valsts informācijas sistēmu, tā ir izvērtējusi, vai tās rīcībā ir valsts informācijas sistēma vai integrētā valsts informācijas sistēma.	**Kritērijs ir sasniegts** Revīzijas apjomā iekļautās iestādes ir izvērtējušas IS atbilstoši MK442 noteiktajiem kritērijiem, iedalot IS pamata vai paaugstinātas drošības sistēmās. Analizējot VIRSIS datus[139] par uzskaitītajām valsts IS, konstatēts, ka: - 64 valsts IS ir reģistrētas kā pamata drošības IS, lai gan no tām 30 ir integrētās IS, līdz ar to revidentu ieskatā būtu nosakāmas kā paaugstinātas drošības IS, jo tās ietekmē visas e-pārvaldes darbības nepārtrauktību; - revīzijas apjomā iekļautās iestādes, reģistrējot datus par valsts IS platformā VIRSIS, 10 gadījumos no 38 IS iestādes ir norādījušas atšķirīgu IS drošības kategoriju, nekā tas ir norādīts iestādes dokumentos.
3.3. Vai normatīvajos aktos ir noteiktas prasības, kā atbilstošo IS pieejamības līmeni sasniegt?	Normatīvie akti paredz prasības, kā nodrošināt IS pieejamības līmeni visām IS.	**Kritērijs nav sasniegts** Normatīvie akti izvirza prasības tikai integrēto valsts IS un savietotāja tehniskās darbības nodrošināšanai, tomēr minētās prasības vairāk ir attiecināmas uz tehniskajiem risinājumiem

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
		IKT infrastruktūras darbības nepārtrauktības nodrošināšanai, nevis konkrēta IS pieejamības līmeņa sasniegšanai. Izvirzītās prasības nenoliedzami sekmē arī IS pieejamības līmeņa nodrošināšanu, tomēr to izpilde pati par sevi negarantē, ka iestāde sasniegs IS (t.sk. e-pakalpojumu) pieejamības līmeni.
	Iestādēm ir pieejama publiska informācija (vadlīnijas, klasifikatori u.tml.), konsultācijas vai labā prakse IKT darbības nepārtrauktības un IS pieejamības nodrošināšanai.	⊗ **Kritērijs nav sasniegts** Nevienā nacionāla līmeņa normatīvajā aktā vai vadlīnijās nav noteikti kritēriji IS un e-pakalpojumu funkcionālajai un pieejamības uzraudzībai, kā arī iestādēm nav pieejamas vienotas, aktuālas, valsts līmenī pārskatītas un patstāvīgai piemērošanai derīgas vadlīnijas vai metodika IS un e-pakalpojumu pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktības novērtēšanai. Lai gan starptautiskā mērogā ir pieejamas dažādas vadlīnijas, standarti un metodikas, galvenokārt IS drošības jomā, kas ietver arī IS pieejamības un IKT darbības nepārtrauktības jautājumus, tomēr revidentu ieskatā būtu nepieciešamas VARAM un AiM apkopotas, izvērtētas un Latvijas videi pielāgotas vadlīnijas, lai iestādes mērķtiecīgi ieviestu organizatoriskos un tehniskos pasākumus, kā arī lai īstenotu IS pieejamības un ar to saistītās IKT infrastruktūras darbības nepārtrauktības pārvaldību.
4. Vai iestādēs tiek nodrošināta IKT darbības nepārtrauktība un vērtēta spēja atjaunot IS darbību incidentu gadījumā?		
4.1. Vai iestādēs ir radīti priekšnoteikumi IS un ar to saistītās IKT infrastruktūras pieejamības un darbības nepārtrauktības nodrošināšanai?		
Vai iestādē ir identificēti būtiskie IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas iesaistīti	Iestādē ir identificēti būtiskie IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas iesaistīti iestādes funkciju izpildes atbalsta nodrošināšanai.	⊘ **Kritērijs sasniegts daļēji** Piecās iestādes ir apzināti IKT resursi (infrastruktūra, IS, programmnodrošinājums, sakaru kanāli), kas ir būtiski iestādes funkciju izpildes atbalsta nodrošināšanā, tomēr pārējās četrās iestādēs būtiskie IKT resursi ir

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
iestādes funkciju izpildes atbalsta nodrošināšanai?		identificēti daļēji, piemēram, identificējot tikai IS. Identificējot tikai IS, iestādē visas izrietošās IKT darbības nepārtrauktības plānošanas darbības ir orientētas tikai uz IS darbības nepārtrauktības plānošanu, kas ir tikai daļa no darbības nodrošināšanā iesaistītajiem IKT resursiem. Turklāt incidentu gadījumā (IKT infrastruktūras vai sakaru pakalpojumu bojājuma gadījumā) iestāde nespēs pietiekami ātri reaģēt un novērst problēmas ar IS nesaistītos resursos.
Vai IS pieejamības prasības ir noteiktas iestādē izstrādātajā IS drošības politikā?	Iestādes IS drošības politika[140]: - Iestādē ir izstrādāta IS drošības politika (pieļaujama kopēja politika visām IS, MK442 8.1., 11.p.); - IS drošības politika tiek pārskatīta reizi gadā vai biežāk, ja ir bijušas būtiskas IS darbības un konfigurācijas izmaiņas vai pēc nozīmīgiem drošības incidentiem (MK442 10.p. ar apakšpunktiem); - IS drošības politika ir izstrādāta atbilstoši MK442 13.punktā minētajām prasībām (MK442. 13.p); - IS drošības politikā noteikti kritēriji: ▪ IS darba laiks (izriet no MK442 7.1.1.–7.1.3.); ▪ IS nepārtrauktās darbības laiks (MK442 13.5.p); ▪ IS pieļaujamais dīkstāves laiks (pieļaujamie dīkstāves laiki ir atbilstoši MK442 un MK421 noteiktajām pieejamības vērtībām; MK442 13.5.p., MK421 9.3.p)); ▪ IS darbības atjaunošanas laiks (MK442 13.5.p.).	⊘ **Kritērijs sasniegts daļēji** Visās revīzijas apjomā iekļautajās iestādēs ir izstrādāta IS drošības politika, tomēr astoņās no deviņām iestādēm tā nebija pilnīga – neietvēra vienu vai vairākas normatīvajā aktā[141] noteiktās prasības, piemēram, nosacījumus, kad ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām. Divos gadījumos – IS drošības politika nav aktualizēta vai pārskatīta, kā to nosaka normatīvais akts.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
Vai iestādē ir veikts būtisko IKT resursu, kas var ietekmēt IS pieejamību un IKT darbības nepārtrauktību, risku novērtējums?	Iestādē ir veikts būtisko IKT resursu risku novērtējums - Sistēmas drošības risku izvērtējums[142]: - Iestādē ir izstrādāta IS drošības risku analīze (IS DRA) (MK442 27.2.p); - IS DRA ietverts būtisko IKT resursu un IS risku izvērtējums. - IS DRA tiek pārbaudīta un atjaunota reizi gadā vai biežāk, ja ir bijušas būtiskas IS darbības un konfigurācijas izmaiņas vai pēc nozīmīgiem drošības incidentiem (MK442 10.p.) - IS DRA ietver (MK442 30.1–30.5.p): ▪ sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu; ▪ institūcijas, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu sistēmas drošības incidents; ▪ sistēmas drošības riska novērtējumu; ▪ sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu; ▪ sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.	**Kritērijs sasniegts daļēji** Divās no deviņām iestādēm nav veikts IS drošības risku novērtējums, 56% iestāžu tas ir veikts atbilstoši normatīvajā aktā noteiktajiem nosacījumiem[143], bet 22% iestāžu – tas ir veikts daļēji.
Vai atbilstoši normatīvajos aktos noteiktajam iestādē ir izstrādāts IS drošības risku pārvaldības plāns?	IS drošības riska pārvaldības plāns (IS DRPP) [144]: - Iestādē ir izstrādāts IS drošības risku pārvaldības plāns (ISDRPP) (MK442 8.4.p); - ISDRPP izstrādāts un aktualizēts, pamatojoties uz IS drošības risku analīzi (MK442 29.p.); - IS DRPP tiek pārbaudīts un atjaunots reizi gadā vai biežāk, ja	**Kritērijs sasniegts daļēji** Trijās no deviņām iestādēm nav izstrādāts IS drošības risku pārvaldības plāns, trijās – tas ir izstrādāts atbilstoši normatīvajā aktā noteiktajiem nosacījumiem[145], bet trijās – tas ir izstrādāts daļēji.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
	ir bijušas būtiskas IS darbības un konfigurācijas izmaiņām vai pēc nozīmīgiem drošības incidentiem (MK442 10.p.); - ISDRPP ir izstrādāts atbilstoši MK442 27.1–27.3.p. minētajām prasībām, ietverot: ▪ veicamās risku analīzes metodoloģijas aprakstu; ▪ sistēmas drošības risku analīzi; ▪ pasākumus sistēmas drošības riska mazināšanai, to izpildes termiņus, finansējumu un par izpildi atbildīgo personu sarakstu.	
Vai atbilstoši normatīvajos aktos noteiktajam iestādē ir izstrādāts IS darbības atjaunošanas plāns?	IS darbības atjaunošanas plāns (IS DAP)[146]: - Iestādē ir izstrādāts IS darbības atjaunošanas plāns (IS DAP) (MK442 8.5.p); - IS DAP ir izstrādāts atbilstoši MK442 33.1–33.4.p. minētajām prasībām, ietverot: ▪ sistēmas IKT resursu atjaunošanas pasākumus, kas veicami pēc sistēmas drošības incidenta; ▪ IS darbības atjaunošanas pasākumu procedūru aprakstu; ▪ IS darbības atjaunošanas pasākumos iesaistīto atbildīgo personu apziņošanas kārtību un darbības instrukcijas; ▪ atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.	⊘ **Kritērijs sasniegts daļēji** Trīs iestādēs no deviņām nav izstrādāts IS darbības atjaunošanas plāns, vienai iestādei tas ir izstrādāts atbilstoši normatīvajā aktā noteiktajiem nosacījumiem[147], bet piecās iestādēs – tas ir izstrādāts daļēji.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
4.2. Vai tiek nodrošināta iestādes uzturēto IS pieejamības uzraudzība?		
Vai iestādēs tiek nodrošināta IS pieejamība atbilstoši normatīvajos aktos vai iestādes noteiktajiem IS pieejamības kritērijiem?	Iestāde nodrošina savu IS pieejamību atbilstoši iestādes noteiktajiem vai normatīvajos aktos noteiktajiem IS pieejamības rādītājiem (pieejamības % no sistēmai noteiktā darbības laika): - integrētajām valsts informācijas sistēmām – 98% pieejamība gada laikā no sistēmai noteiktā darbības laika (MK421 9.3.p); - savietotājam – 99% pieejamība gada laikā no sistēmai noteiktā darbības laika (MK421 9.3.p); - visām pārējām iestādes IS – iestādes noteiktā IS pieejamība % no sistēmu darbības laika.	**Kritērijs sasniegts daļēji** Neviens normatīvais akts neparedz informācijas par e-pakalpojumu un to atbalstošo IS pieejamību apkopošanu. Tikai trīs no revīzijas apjomā iekļautajām iestādēm ir mērījušas faktiski sasniegto IS pieejamības līmeni savām uzturētajām IS – šīs iestādes informēja, ka, lai gan dažos mēnešos pieejamība kādai IS vai e-pakalpojumam ir pazeminājusies zem 98%, tomēr gada griezumā visām IS tiek pārsniegta 98% pieejamība. Pārējās revīzijas apjomā iekļautās iestādes (sešas iestādes) vai nu nesniedza datus, vai nu norādīja, ka to rīcībā nav datu par IS pieejamības rādītājiem. Iestādes skaidro, ka to rīcībā nav tāda rīka (automatizēta uzraudzības risinājuma) un nav izvirzītu uzraugāmo kritēriju, ar kuru palīdzību uzkrāt datus un noteikt IS pieejamību. Šīs iestādes uzskata, ka sasniedz noteiktos pieejamības radītājus, pamatojot to ar faktu, ka gada laikā nav konstatēti būtiski IS drošības incidenti, tomēr ticamus un viennozīmīgi interpretējamus datus par sasniegto IS pieejamības līmeni iestādes nevar iesniegt – attiecīgi nav nosakāms, vai šo iestāžu IS sasniedz noteikto IS pieejamības līmeni. Attiecībā uz e-pakalpojumu pieejamības nodrošināšanu saskaņā ar revidentu veikto analīzi par portālā Latvija.lv publicētajiem paziņojumiem par portāla un e-pakalpojumu darbības traucējumiem 2021. gada oktobrī un laikā no 2022. gada janvāra līdz martam, konstatēts, ka kopumā par 21 e-pakalpojumu (jeb 17% no visiem Latvija.lv esošajiem e-pakalpojumiem) ir bijuši paziņojumi, ka e-pakalpojums nedarbojas, no tiem astoņi e-pakalpojumi nedarbojās no vienas līdz 23 dienām, tādējādi secināms, ka tie konkrētajā mēnesī ir bijuši pieejami robežās no 26% līdz 96,8%, kas ir mazāk nekā normatīvajā aktā noteiktais 98% sasniedzamais e-pakalpojuma līmenis.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
Vai tiek nodrošināts monitorings IKT resursu kritiskajām robežām (procesora noslodze, RAM noslodze, datu kanālu noslodze) un IS veiktspējai?	Iestāde veic ikdienas monitoringu (uzraudzību) IKT resursu kritiskajām robežām (procesora noslodze, RAM noslodze, datu kanālu noslodze), kā arī IS veiktspējai[148] (MK421 8.1. un 8.3p.).	**Kritērijs ir sasniegts** Visās iestādēs ikdienas IS un IKT infrastruktūras darbības uzraudzībai tiek izmantoti dažādi monitoringa rīki. [IP].
Vai tiek nodrošināta IKT infrastruktūras darbību ietekmējošo vides drošības elementu uzraudzība?	Iestāde veic savas IKT infrastruktūras darbību ietekmējošo vides drošības elementu uzraudzību: - tiek nodrošināta nepārtraukta elektroenerģijas padeve un uzraudzīta UPS iekārtu darbība; - UPS iekārtas ir pārbaudītas, vai spēj nodrošināt strāvas padevi līdz 30 min[149] (MK421 3.1.p.); - darbojas ugunsdrošības signalizācija, tā tiek testēta; - tiek uzraudzīts mikroklimats (mitrums, temperatūra) serveru telpās; - mikroklimata iekārtām tiek nodrošināta apkope.	**Nav vērtēts.** Ņemot vērā Covid-19 pandēmijas apstākļus, revīzijā netika veiktas detalizētas revīzijas apjomā iekļauto iestāžu serveru telpu pārbaudes klātienē, paļaujoties uz iestāžu sniegto informāciju par IKT infrastruktūras darbību ietekmējošu vides drošības elementu uzraudzību. Revīzijas laikā visas iestādes norādīja, ka tās nodrošina serveru telpu aizsardzību pret fiziskiem apdraudējumiem (t.sk. neatbilstošiem klimatiskajiem apstākļiem, ugunsgrēku, plūdiem, elektroenerģijas padeves pārtraukumiem, tīšiem bojājumiem)
4.3. Vai, nododot ārpakalpojumā, tiek nodrošināta IS pieejamība?	- Līgumos ar ārpakalpojuma sniedzējiem ir ietvertas prasības IS pieejamības un IKT darbības nepārtrauktības nodrošināšanai (MK442 20.2 punkts, 20.3.2. punkts).	**Kritērijs sasniegts daļēji** Četras no deviņām revīzijas apjomā iekļautajām iestādēm ir noslēgušas ārpakalpojuma līgumus par iestādes IS vai ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanu, bet nevienā no tiem nav ietvertas skaidras un nepārprotamas prasības IS un ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanai un ziņošanai par faktiski sasniegto pieejamības līmeni. Piemēram, līgumā starp iestādi un ārpakalpojuma sniedzēju ir noteikts iestādes IS darbības laiks (darba laiks), bet nav noteikts pieejamības līmenis, kas ārpakalpojuma sniedzējam ir jānodrošina.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
		Sasniedzamais IS pieejamības līmenis nav līgumā paredzēts, lai gan normatīvais akts[150] izvirza, piemēram, integrētajām valsts IS nodrošināt pieejamības līmeni 98% gadā.
	- Iestāde uzrauga līgumos ar ārpakalpojuma sniedzējiem ietverto prasību izpildi saistībā ar IS pieejamības un IKT darbības nepārtrauktības nodrošināšanu (MK442 20.3.1. un 20.3.4.punkts).	**Kritērijs sasniegts daļēji** Trīs no četrām iestādēm neveic regulāru ārpakalpojuma līgumos par IS un ar to saistītās IKT infrastruktūras darbības nepārtrauktības un pieejamības nodrošināšanu iekļauto prasību izpildes uzraudzību.
4.4. Vai valsts piedāvā iestādēm risinājumus IKT darbības nepārtrauktības un IS pieejamības uzlabošanai?	Valsts piedāvā iestādēm risinājumus IKT darbības nepārtrauktības un IS pieejamības uzlabošanai – piedāvātie risinājumi iestādēs var tikt izmantoti bez ierobežojumiem (piemēram, bez lielām izmaksām risinājumu ieviešanai vai uzturēšanai).	**Kritērijs sasniegts daļēji** CERT.LV ir izveidojis[151] sensoru tīklu, kas nodrošina datu plūsmas anomāliju analīzi, ļaunatūras atpazīšanu un brīdinājumu saņemšanu par konstatētajiem apdraudējumiem iestādes datortīklā. Saskaņā ar CERT.LV sniegto informāciju pašlaik ir uzstādīti [IP] šādi sensori, tomēr CERT.LV nenorāda, cik plaša elektroniskā telpa ar tiem tiek monitorēta. [IP]

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
4.5. Vai nodrošināta IKT darbības nepārtrauktība un spēja atjaunot IS pieejamību incidentu gadījumā?		
Vai iestāžu IKT stratēģijās un darbu plānos ir iekļauti IS pieejamības jautājumi?	Iestādē ir izstrādāta IKT darbības politika vai IKT stratēģija ar ietvertiem mērķiem IKT darbības nepārtrauktības nodrošināšanā un sasniedzamajiem kritērijiem IS pieejamībā. Iestādes darbu plānos ietverti uzdevumi IKT darbības nepārtrauktības un IS pieejamības nodrošināšanai.	**Kritēriji sasniegti daļēji** No revīzijas apjomā iekļautajām iestādēm trijās iestādēs IKT darbības nepārtrauktības un IS pieejamības jautājumi ir ietverti iestādes darbības vai IKT stratēģijās, kā arī pakārtotajos darbu plānos, pārējās sešās iestādēs, nenosakot mērķus un uzdevumus IS pieejamības nodrošināšanai, IS pieejamība nav apzināta kā būtiska nepieciešamība iestādes funkciju nodrošināšanai.
Vai iestādē tiek vērtēti IKT darbības nepārtrauktības incidenti un tiek mērīta sasniegtā IS pieejamība?	Iestāde vērtē IKT darbības nepārtrauktības incidentus un nodrošinātos IS pieejamības rezultātus ar mērķi samazināt konkrēto incidentu iestāšanos varbūtību nākotnē un palielināt IS pieejamību.	**Kritērijs sasniegts daļēji** Visās revīzijas apjomā iekļautajās iestādēs ir noteiktas procedūras IKT incidentu izvērtēšanai un informācija par IKT incidentiem pēc iespējas tiek iekļauta ikgadējā iestādes IKT risku analīzē. Jānorāda, ka iestāžu incidentu reģistru dati ir nepilnīgi – sešas iestādes no deviņām revīzijas apjomā iekļautajām iestādēm ir norādījušas, ka neuzrauga e-pakalpojumu pieejamību, līdz ar to var būt gadījumi, kad pārtraukumi e-pakalpojuma darbībā netiek fiksēti un reģistrēti, savukārt divas iestādes neiesniedza incidentu reģistra datus, liedzot novērtēt, vai šo iestāžu incidentu reģistros tiek uzkrāta informācija par incidentiem, kas būtu varējuši ietekmēt iestāžu IS darbības nepārtrauktību un sasniedzamo IS pieejamības līmeni. Attiecībā uz sasniegtās IS pieejamības mērīšanu – tikai trīs no revīzijas apjomā iekļautajām iestādēm ir mērījušas faktiski sasniegto IS pieejamības līmeni savām uzturētajām IS, savukārt pārējās revīzijas apjomā iekļautās iestādes (sešas iestādes) vai nu nesniedza datus, vai nu norādīja, ka to rīcībā nav datu par IS pieejamības rādītājiem.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
Vai iestāde iespējami īsā laikā nodrošina IKT darbības un IS pieejamības atjaunošanu incidentu gadījumā?		
▪ Vai IKT darbības atjaunošanas plāns (IKT DAP) ir testēts?	IS DAP tiek pārbaudīts (testēts) un atjaunots reizi gadā vai biežāk, ja ir bijušas būtiskas IS darbības un konfigurācijas izmaiņas vai pēc nozīmīgiem drošības incidentiem (MK442 10.p.)	**Kritērijs sasniegts daļēji** No revīzijas apjomā iekļautajām deviņām iestādēm sešās iestādēs ir izstrādāti IS darbības atjaunošanas plāni, bet trīs iestādēs ne reizi vēl nav pārbaudīts izstrādātais IS darbības atjaunošanas plāns pilnā apmērā.
▪ Vai incidentu gadījumos IKT pakalpojumi un IS tiek atjaunotas IKT DAP noteiktajos laikos un apjomā?	Incidentu gadījumos IKT pakalpojumi un IS tiek atjaunotas IKT DAP noteiktajos laikos un apjomā.	**Kritērijs sasniegts daļēji** Saskaņā ar iestāžu sniegto informāciju 2021.gadā to IS nav novēroti tādi būtiski IKT incidenti, lai būtu bijusi jāatjauno IS darbība. No sešām iestādēm, kuras ir izstrādājušas IS darbības atjaunošanas plānus: - trīs iestādēs, veicot IKT DAP pārbaudes, IS ir izdevies atjaunot IKT DAP noteiktajos laikos un apjomā; - trijās iestādēs ne reizi nav veiktas pārbaudes, vai IKT DAP ietvertās procedūras IKT infrastruktūras, IS programmatūras, datu bāzu, IS servisu un e-pakalpojumu darbības atjaunošanai ir pilnīgas un pietiekamas, lai iespējami īsā laikā atjaunotu IS pieejamību.
▪ Vai ir nodrošinātas apmācības darbiniekiem IKT darbības nepārtrauktības nodrošināšanā?	Tiek nodrošinātas apmācības darbiniekiem IKT darbības nepārtrauktības nodrošināšanā.	**Kritērijs nav sasniegts** No revīzijas apjomā iekļautajām deviņām iestādēm tikai vienā iestādē nodrošinātas apmācības darbiniekiem IKT darbības nepārtrauktības nodrošināšanā. Pārējās iestādēs atkarībā no IT struktūrvienības darbinieka specializācijas tiek organizētas apmācības par IS administrēšanas un IKT infrastruktūras uzturēšanas jautājumiem kopumā, bet neietverot IS darbības atjaunošanas simulāciju.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
▪ Vai iestādē tiek nodrošināta datu rezerves kopiju veidošana, glabāšana un datu atjaunošana?	Datu rezerves kopēšana, glabāšana un atjaunošana: - iestāde nodrošina datu rezerves kopiju veidošanu (MK442 15.17. p.); - iestāde nodrošina datu rezerves kopiju atjaunošanu (MK442 15.17. p.); - integrētajām valsts informācijas sistēmām un savietotājam rezerves kopijas (pilnās un pieauguma) tiek veidotas un pārbaudītas atbilstoši MK421 noteiktajām prasībām (MK421 10.6.p); - *rezerves kopiju veidošanas un atjaunošanas kārtība*[154] (MK421 25.4.p): ▪ izstrādāta IS rezerves kopiju izgatavošanas un glabāšanas kārtība; ▪ izstrādāta kārtība, kā pārbaudīt, vai no rezerves kopijām var atjaunot datus. - *rezerves kopiju glabāšana*[155] (MK421 10.1–10.5.): ▪ pilnās rezerves kopijas tiek glabātas ģeogrāfiski nošķirtā vietā; ▪ rezerves kopiju glabāšanas ilgums atbilst MK421 prasībām (no 1 mēn. līdz 3 gadi); ▪ nedēļas, mēneša un gada kopijas tiek glabātas vietā, kurā netiek pieļauta trešo personu piekļuve un bojājumi ugunsgrēku, plūdu u.c. gadījumos.	**Kritērijs sasniegts daļēji** Visās revīzijas apjomā iekļautajās iestādēs tiek nodrošināta datu rezerves kopiju veidošana un nepieciešamības gadījumā arī datu atjaunošana no rezerves kopijas, tomēr tikai Piecās no deviņām ir izstrādāta datu rezerves kopiju veidošanas kārtība un četrās – kārtība datu atjaunošanai no rezerves kopijām. Lai gan integrētajām valsts IS testa vidē ne retāk kā reizi kalendāra gadā[156] ir jāveic kopiju atjaunošanas pārbaudes, tomēr sešas no deviņām iestādēm to nenodrošina, jo iestādes paļaujas uz rezerves kopiju veidošanas programmatūru iebūvētajām automatizētām kontrolēm vai pārbaudi veic tikai pēdējai pilnajai kopijai. Lai gan visas iestādes norādīja, ka datu rezerves kopijas tiek glabātas ģeogrāfiski nošķirtā vietā, tomēr septiņas no deviņām iestādēm datu rezerves gada kopijas glabā mazāku termiņu, nekā noteikts normatīvajā aktā[157].

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
5. Vai vienkopus tiek uzkrāti dati, lai mērītu, vai IS pieejamība tiek sasniegta un kādas sekas izraisa IS nepieejamība?		
	Valstī vienkopus tiek uzkrāti un analizēti dati par IS nepieejamības gadījumiem.	**Kritērijs sasniegts daļēji** Nacionālā līmenī informāciju par iestādēs notikušajiem IKT darbības incidentiem uzkrāj CERT.LV, tomēr par visiem notikušajiem incidentiem, kas ietekmē un var apdraudēt IS pieejamību, CERT.LV informāciju nesaņem. CERT.LV statistikā par notikušajiem drošības incidentiem netiek uzkrāta informācija par to, kādas IS incidents ir ietekmējis.
	Uzkrātā informācija par IS nepieejamības gadījumiem tiek vērtēta, lai veiktu nepieciešamās darbības, kas samazinātu konkrētā incidenta iestāšanās varbūtību nākotnē.	**Kritērijs sasniegts daļēji** CERT.LV analizē IT drošības incidentus, tostarp tādus, kuri ir izraisījuši IS darbības traucējumus, tomēr valstiskā līmenī šī informācija netiek tālāk analizēta. Revidentu ieskatā, valstiskā līmenī analizējot datus ne tikai par valstī notiekošajiem IKT incidentiem, bet arī par visiem IS nepieejamības gadījumiem vai darbības traucējumiem, jau valstiskā mērogā varētu nodrošināt preventīvu rīcību, kas būtu vērsta uz iepriekš bijušu incidentu un cēloņu, kas ietekmē IKT darbības nepārtrauktību un IS pieejamību, rašanās iespējamības samazināšanu vai pat novēršanu nākotnē. Iestāžu incidentu reģistru dati ir nepilnīgi – 75% iestāžu no revīzijas apjomā iekļautajām iestādēm ir norādījušas, ka neuzrauga e-pakalpojumu pieejamību, līdz ar to var būt gadījumi, kad pārtraukumi e-pakalpojuma darbībā netiek fiksēti un reģistrēti.

Revīzijas jautājums / apakšjautājums	Noteiktais kritērijs	Kritērijs ir sasniegts / nav sasniegts / sasniegts daļēji
	Valstī tiek analizēts, vai kopumā tiek sasniegta IS pieejamība.	**Kritērijs nav sasniegts** Lai gan prasības sasniedzamajam pieejamības līmenim integrētajām valsts IS un savietotājam ir izvirzītas kopš 2012.gada, e-pakalpojumiem – kopš 2017.gada, tomēr valsts pārvaldē nav veikta analīze, kāds ir faktiski sasniegtais e-pakalpojumu un to atbalstošo IS pieejamības līmenis. Nav arī noteikta atbildīgā iestāde, kurai šādas informācijas apkopošana un analīze būtu jāveic.
	Valstī tiek analizēts, cik lielus zaudējumus rada IS nepieejamība.	**Kritērijs nav sasniegts** Latvijā līdz šim nav veiktas aplēses, cik daudz ir izmaksājusi IS nepieejamība un kādas sekas tas ir radījis privātpersonām vai plašāk – tautsaimniecībai. Piemēram, saskaņā ar CERT.LV apkopoto informāciju[158] par IS drošības incidentiem valsts pārvaldē vienā no incidentiem vien tika ietekmēta [IP] valsts un pašvaldību iestāžu vietņu darbība. Turklāt IS nepieejamības gadījumā sekas varēja rasties ne tikai pašai iestādei, bet arī citām iestādēm, kuras savlaicīgi nesaņēma nepieciešamo informāciju un nevarēja sniegt pakalpojumus. E-pakalpojuma nepieejamība rada sekas gan privātpersonai, kurai ir jāmeklē alternatīvs risinājums pakalpojuma saņemšanai vai jātērē laiks, pārbaudot, vai pakalpojuma pieejamība ir atjaunota, gan arī valsts pārvaldei, apkalpojot privātpersonu mazāk automatizētā pakalpojumu sniegšanas kanālā. Saskaņā ar revīzijā veikto aplēsi e-pakalpojuma nesaņemšana attālināta veidā privātpersonai var radīt 15,40 *euro* izmaksas un var nākties patērēt 1,5 stundu laika, lai to saņemtu klātienē, kā arī nelietderīgi tērē iestādes resursus 1,83 *euro* apmērā par vienu pakalpojumu. Kopumā attiecībā uz revīzijā konstatētajiem 10 tūkst. pakalpojumu nepieejamības gadījumiem varēja tikt radītas izmaksas iedzīvotājiem 162 tūkst. *euro* un valsts pārvaldei – 19,2 tūkst. *euro* apmērā, ko varēja izmantot efektīvāk citu funkciju veikšanai.

Revīzijas metodes

Revīzijā izmantotas šādas galvenās metodes:

- analizēti attīstības plānošanas dokumenti, normatīvie akti un citi ar revidējamo jomu saistīti dokumenti un informācija;
- vērtēta un analizēta iestāžu iesniegtā informācija par IKT darbības nepārtrauktības nodrošināšanu, sasniegtā IS un e-pakalpojumu pieejamības līmeņa novērtēšanu;
- pēc revidentu izveidotās vērtējumu metodikas veikts izvērtējums par iestādēs ieviestajiem priekšnoteikumiem IS pieejamības un IKT darbības nepārtrauktības nodrošināšanai;
- intervētas iestāžu atbildīgās personas.

Sektora vadītāja I.Kalniņa-Junga

Departamenta direktore I.Bādere

ŠIS DOKUMENTS IR ELEKTRONISKI
PARAKSTĪTS AR DROŠU ELEKTRONISKO
PARAKSTU UN SATUR LAIKA ZĪMOGU

Saīsinājumi

Saīsinājums	Skaidrojums
AiM	Aizsardzības ministrija
CERT.LV	Informācijas tehnoloģiju drošības incidentu novēršanas institūcija; Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā IT drošības likuma ietvaros
IKT	Informācijas un komunikācijas tehnoloģijas
IT	Informācijas tehnoloģijas
IS	Informācijas sistēma
VARAM	Vides aizsardzības un reģionālās attīstības ministrija
BVKB	Būvniecības valsts kontroles birojs
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]
[IP]	[IP]

Saīsinājums	Skaidrojums
[IP]	[IP]
MK442	Ministru kabineta 28.07.2015. noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"
MK421	Ministru kabineta 19.06.2012. noteikumi Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības"
MK402	Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi"
MK400	Ministru kabineta 04.07.2017. noteikumu Nr.400 "Valsts pārvaldes pakalpojumu portāla noteikumi"
MK560	Ministru kabineta 19.09.2017. noteikumu Nr.560 "Noteikumi par kvalificēta un kvalificēta paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzēja un tā sniegtā pakalpojuma tehniskajām un organizatoriskajām prasībām"
ES/EEZ	Eiropas Savienības/Eiropas Ekonomikas zonas valstis
UPS	Elektroenerģijas nepārtrauktās barošanas bloki

Atsauces

[1] Valsts kases Valsts budžeta un pašvaldību budžeta pārskatu sistēmas dati par izlietoto finansējumu (*euro*) IT pakalpojumiem: 2017. gadā – 41135463, 2018. gadā – 47372778, 2019. gadā – 48163508, 2020. gadā – 52967430, 2021. gadā - 64129828.

[2] CERT.LV 2021. gada 4. ceturkšņa "Publiskais pārskats par CERT.LV uzdevumu izpildi" (interneta resurss: https://cert.lv/uploads/parskati/cert-ceturksna-C4-atskaite-2021-LV.pdf; resurss skatīts 01.06.2022.)

[3] Analīze veikta par 2021.gada oktobrī un laikā no 2022.gada janvāra līdz martam.

[4] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.1., 8.4., 8.5., 27.2. apakšpunkti.

[5] Labā prakse – COBIT, ITIL.

[6] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.6. apakšpunkts.

[7] "Latvijas Nacionālais attīstības plāns 2021.–2027.gadam (apstiprināts ar Latvijas Republikas Saeimas 2020.gada 2.jūlija lēmumu Nr.418/Lm13), "Digitālās transformācijas pamatnostādnes 2021.–2027.gadam" (pieņemtas Ministru kabinetā 2021.gada 6.jūlijā), informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022.gadam" (apstiprināts Ministru kabinetā 2019.gada 17.septembrī).

[8] Revidenta aplēse: Vienas stundas administratīvais slogs portālam Latvija.lv * četras stundas mēnesī = 16 tūkst. *euro/h* * 4 h = 64 tūkst. *euro*

[9] Ministru kabineta 04.07.2017. noteikumu Nr.399 "Valsts pārvaldes pakalpojumu uzskaites, kvalitātes kontroles un sniegšanas kārtība" 2.1. apakšpunkts.

[10] IKT uzturēšanai izlietotais finansējums (*euro*) pa gadiem pēc Valsts Kases VBPBP IS datiem: 2017. gadā 41135463, 2018. gadā 47372778, 2019. gadā 48163508, 2020. gadā 52967430, 2021. gadā 64129828.

[11] Rokasgrāmatas augstākajām revīzijas iestādēm "*WGITA – IDI Handbook on IT audit for supreme audit institutions*" (apstiprināta XXI INCOSAI kongresā 2013.gada oktobrī, Pekinā, Ķīnā), nodaļas "*I.3 Key elements of Information Security*" sadaļa "*a. Information Security Environment*".

[12] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[13] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.

[14] Portāla Latvija.lv sadaļa "Par portālu" (interneta resurss: https://latvija.lv/lv/ParPortalu; interneta resurss skatīts: 01.11.2021.)

[15] E-pakalpojumu statistika portālā Latvija.lv (interneta resurss: https://latvija.lv/Meklesana?f_abc_lvp_categoryTypes=ExternalEService~PortalEService, interneta resurss skatīts: 01.05.2022.)

[16] Informācijas tehnoloģiju drošības likuma 8.panta pirmā daļa; Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 10. punkts.

[17] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 6. punkts.

[18] 2019.gada Valsts kontroles lietderības revīzija "Vai valsts pārvaldē tiek noteikta vienota IKT infrastruktūras pārvaldība, lai nodrošinātu tās efektīvu izmantošanu?".

[19] Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022.gadam" (apstiprināts Ministru kabinetā 2019.gada 17.septembrī, protokols Nr.42, 43.§)

[20] "Digitālās transformācijas pamatnostādnes 2021-2027.gadam" (atbalstītas ar Ministru kabineta 07.07.2021. rīkojumu Nr.490).

[21] "Latvijas Nacionālais attīstības plāns 2021.-2027.gadam (apstiprināts ar Latvijas Republikas Saeimas 2020.gada 2.jūlija lēmumu Nr.418/Lm13).

[22] Ministru kabineta 19.03.2011. noteikumu Nr.233 "Vides aizsardzības un reģionālās attīstības ministrijas nolikums" 1.7., 4.1.8., 5.7. apakšpunkti.

[23] Ministru kabineta 19.03.2011. noteikumu Nr.233 "Vides aizsardzības un reģionālās attīstības ministrijas nolikums" 5.7.4. apakšpunkts.
[24] Ministru kabineta 29.04.2003. noteikumu Nr.236 "Aizsardzības ministrijas nolikums" 5.15.[1] apakšpunkts; Aizsardzības ministrijas 06.02.2017. reglaments Nr.1 REGL "Krīzes vadības departamenta nolikums".
[25] Informācijas tehnoloģiju drošības likuma 4. un 5.pants.
[26] Revidenta aplēse: portāla Latvija.lv kopējais izmantošanas skaits gadā/365 dienām = 8 222 489 izmantošanas reizes/365 dienām = 22 500 reizes/dienā.
[27] Revidenti ieguva informāciju par portālā Latvija.lv publicētajiem paziņojumiem 2021. gada oktobrī, 2022. gada janvārī, februārī un martā.
[28] "*Costs of Unavailability*" (interneta resurss: https://www.seriosoft.com/blog/costs-unavailability; resurss skatīts:16.04.2021.)
[29] *Information Technology Intelligence Consulting Corp.* pētījuma "*ITIC 2020 Global Server Hardware, Server OS Reliability Report"* dati par IKT infrastruktūras un serveru operētājsistēmu uzticamību 2020.gadā (interneta resurss: https://www.ibm.com/downloads/cas/DV0XZV6R#:~:text=To%20obtain%20the%20most%20accurate,ITIC%20accepts%20no%20vendor%20sponsorship.&text=exceed%20%24150%2C000%20and%2088%25%20of,over%20one%20million%20(%241%2C000.000) , resurss skatīts:19.05.2022.)
[30] 2011.gada Valsts kancelejas "Rokasgrāmata „Paplašinātais standarta izmaksu modelis"" 13.lpp.
[31] 2011.gada Valsts kancelejas "Rokasgrāmata „Paplašinātais standarta izmaksu modelis"" sadaļas "7.solis. Standarta izmaksu parametru noteikšana" un "8.solis "Administratīvā sloga aprēķins"
[32] Iestādēs veiktās revidentu aptaujas "Par IS, kurās informācijas apmaiņa notiek ar citām valstīm" dati.
[33] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.
[34] Informācijas tehnoloģiju drošības likums, Ministru kabineta 28.07.2015. noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām", Ministru kabineta 19.06.2012. noteikumi Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības".
[35] Ministru kabineta 04.07.2017. noteikumi Nr.399 "Valsts pārvaldes pakalpojumu uzskaites, kvalitātes kontroles un sniegšanas kārtība", Ministru kabineta 04.07.2017. noteikumi Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi".
[36] Valsts pārvaldes iekārtas likuma 10.panta sestā daļa.
[37] Ministru kabineta 04.07.2017. noteikumu Nr.399 "Valsts pārvaldes pakalpojumu uzskaites, kvalitātes kontroles un sniegšanas kārtība" 23. punkts un 24.punkts.
[38] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 7. punkts.
[39] Statistika pieejama Atvērto datu portālā sadaļā "Pakalpojumu uzskaites statistika" (interneta resurss: https://data.gov.lv/dati/lv/dataset/pakalpojumu-uzskaites-statistika-par-2019-gadu/resource/e0490c47-6b3c-4f5a-b871-96c378ac3763, resurss skatīts: 23.05.2022.)
[40] E-pakalpojums iestādes mājas lapā un e-pakalpojumi portālā Latvija.lv.
[41] E-pasts un citi elektroniskie kanāli.
[42] Telefons, fakss, pasts, sms un citi kanāli.
[43] Klātienē iestādē vai valsts un pašvaldību vienotajos klientu apkalpošanas centros (VPVKAC).
[44] Valsts reģionālās attīstības aģentūras 02.09.2021. intervijā Valsts kontrolei sniegtā informācija.
[45] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 13.4 un 15.1. apakšpunkts, Ministru kabineta 04.07.2017. noteikumu Nr.400 "Valsts pārvaldes pakalpojumu portāla noteikumi" 18.1.1. punkts, VRAA 26.03.2019. iekšējie noteikumu Nr. 1-2/19/6 "Valsts informācijas sistēmu savietotāja infrastruktūras pakalpojumu lietošanas noteikumi" 24.8. un 24.9.2. apakšpunkts.
[46] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.
[47] Informācijas tehnoloģiju drošības likuma 5.panta pirmā daļa.
[48] [IP]
[49] Revidenta aplēse: portāla Latvija.lv kopējais izmantošanas skaits gadā/365 dienām = 8 222 489 izmantošanas reizes/365 dienām = 22 500 reizes/dienā.
[50] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.
[51] Portālam Latvija.lv noteiktais darbības laiks 24/7, izmantošanas reižu skaits – 8 222 489 reizes (gadā) jeb 2 055 622 reizes ceturksnī.

[52] E-pakalpojumu, portāla Latvija.lv lietošanas dati – dati par 2021. gada janvāri – martu vai 2021. gadu.

[53] Paziņojumi portālā Latvija.lv: "Iespējami portāla un e-pakalpojumu darbības traucējumi tehnisku iemeslu dēļ", "LRVTC tehnisko darbu dēļ var būt traucējumi PMLP un Rīgas Domes e-pakalpojumos", "Saistībā ar tehniskajiem darbiem PMLP, iespējami darbības traucējumi PMLP un citu iestāžu e-pakalpojumos".

[54] Paziņojumi portālā Latvija.lv: "Saistībā ar tehnisko darbu veikšanu var tikt traucēta autentifikācija portālā", "Var tik traucēta juridiskās personas autentifikācija Latvija.lv (saistībā ar plānotu UR infrastruktūras maiņu)", "Tehnisku iemeslu dēļ nav iespējams autorizēties, izmantojot Swedbank Smart-ID autentifikāciju", "LVRTC tehnisko darbu dēļ var būt traucējumi juridisko personu autentifikācijā".

[55] Paziņojumi portālā Latvija.lv: "Tehnisku iemeslu dēļ iespējami traucējumi maksājumu veikšanā ar Swedbank banku", "Traucējumi maksājumu veikšanā", "Saistībā ar tehniskajiem darbiem PMLP, iespējami darbības traucējumi maksājumu veikšanā".

[56] Paziņojumi portālā Latvija.lv: "Var būt traucēta e-adreses ziņojumu parakstīšana", "Tehnisku iemeslu dēļ personas, kuras portālā autorizējas kā pilnvarotās personas, nevar piekļūt fiziskas vai juridiskas personas e-adreses informācijai (t.sk. traucēta e-adreses ziņojumu skatīšana, dzēšana)".

[57] Portālam Latvija.lv noteiktais darbības laiks 24/7, izmantošanas reižu skaits – 8 222 489 reizes (gadā) jeb 2 055 622 reizes ceturksnī.

[58] E-pakalpojumu, portāla Latvija.lv lietošanas dati – dati par 2021.gada janvāri – martu vai 2021. gadu.

[59] VZD e-pakalpojumi: "Mani dati Kadastrā", "Datu atlase un izvade par konkrētiem objektiem vai apgabaliem pēc definētiem parametriem", "Valsts zemes dienestā reģistrēto pasūtījumu statusu izsekošana un jaunu pasūtījumu noformēšana", "Valsts zemes dienesta tematisko karšu pārlūkošana".

[60] Aplēsē izmantoti dati par PMLP e-pakalpojumiem "Dzīvesvietas deklarācijas iesniegšana" un "Iesniegums par dzīvesvietas reģistrēšanu ārvalstīs", jo no 2021. gada 1. janvāra šie e-pakalpojumi tikai apvienoti vienā e-pakalpojumā "Dzīvesvietas deklarēšana vai norādīšana".

[61] VSAA e-pakalpojumi: "Informācija par prognozējamo vecuma pensijas apmēru", "Informācija par izmaksai nosūtīto pensiju, pabalstu, atlīdzību", "Informācija par izmaksai nosūtīto pensiju, pabalstu, atlīdzību", "Informācija par pensiju 1.līmeņa kapitālu", "Informācija par dalību pensiju 2. līmenī", "Informācija par reģistrēto darba stāžu līdz 1996.gadam", "Informācija par ieturējumiem no VSAA veiktajiem maksājumiem", "Informācija par ieturēto ienākuma nodokli no pensijas vai pabalsta", "Darba devēja E-iesniegums sociāli apdrošināmās personas statusa saglabāšanai Latvijā, parasti strādājot divās vai vairākās ES/EEZ valstīs vai Šveicē".

[62] VARAM aplēse par nepieciešamo pakalpojuma apkalpošanas laiku klātienē. Dati no VARAM 2016.gada Eiropas Reģionālās attīstības fonda projekta iesnieguma projektam Nr. 2.2.1.1/16/I/001 "Publiskās pārvaldes informācijas un komunikācijas tehnoloģiju arhitektūras pārvaldības sistēma (PIKTAPS)".

[63] Informācija par vidējo atalgojumu Latvijā 2022.gada 1.ceturksnī (Interneta resurss: https://www.lsm.lv/raksts/zinas/ekonomika/latvija-videja-alga-uz-papira-ceturksna-griezuma-sarukusi-par-29.a459157/ , resurss skatīts: 31.05.2022.)

[64] VARAM aplēse par iedzīvotāja laika patēriņu iestādes apmeklējumam klātienē. Dati no VARAM 2016.gada Eiropas Reģionālās attīstības fonda projekta iesnieguma projektam Nr. 2.2.1.1/16/I/001 "Publiskās pārvaldes informācijas un komunikācijas tehnoloģiju arhitektūras pārvaldības sistēma (PIKTAPS)".

[65] Informācija par vidējo atalgojumu Latvijā 2022.gada 1.ceturksnī (Interneta resurss: https://www.lsm.lv/raksts/zinas/ekonomika/latvija-videja-alga-uz-papira-ceturksna-griezuma-sarukusi-par-29.a459157/ , resurss skatīts: 31.05.2022.)

[66] Rīgas pašvaldības SIA "Rīgas satiksme" biļetes cena diviem braucieniem sabiedriskajā transportā (interneta resurss: https://www.rigassatiksme.lv/lv/biletes/bilesu-klasts-un-cenas-1/bilete-noteiktam-braucienu-skaitam/; resurss skatīts: 01.06.2022.)

[67] Revidenta aplēse: portāla Latvija.lv kopējais izmantošanas skaits dienā (22 500 reizes) * administratīvā sloga izmaksas par katru pakalpojuma nesaņemšanas reizi (17,23 *euro)* = 387 tūkst. *euro*

[68] Informācijas tehnoloģiju drošības likuma 6. panta otrā daļa.

[69] Informācijas tehnoloģiju drošības likuma 6. panta pirmā daļa.

[70] Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) mājas lapa, sadaļa "Kad ziņot par incidentu vai drošības nepilnību?" (resurss: https://cert.lv/lv/valsts-un-pasvaldibu-iestadem/kad-zinot-par-incidentu-vai-drosibas-nepilnibu , resurss skatīts: 16.02.2021.).

[71] Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) mājas lapa, sadaļa "Kad ziņot par incidentu?" (interneta resurss: https://cert.lv/lv/kad-zinot-par-incidentu, resurss skatīts: 12.05.2022.)

[72] Ministru kabineta 15.01.2019. noteikumi Nr.15 "Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu".

[73] Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) mājas lapa – Informācija par CERT.LV sensoru tīklu (Agrīnās brīdināšanas sistēmu) (interneta resurss: https://cert.lv/lv/pamatpakalpojumu-un-digitalo-pakalpojumu-sniedzejiem, resurss skatīts 12.02.2021.)

[74] [IP]

[75] [IP]

[76] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[77] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.

[78] Revidenta aplēse: Vienas stundas administratīvā sloga izmaksas portālam Latvija.lv * četras stundas mēnesī = 16 tūkst. *euro/h* * 4 h = 64 tūkst. *euro*

[79] *European Commission* 23.12.2020. *Commission staff working document "Customs 2020 Programme Progress Report 2019"* (interneta resurss: https://ec.europa.eu/taxation_customs/sites/taxation/files/customs_programme_progress_report_2019.pdf.pdf, resurss skatīts:12.04.2021.)

[80] *European Commission 23.12.2020. Commission staff working document "Customs 2020 Programme Progress Report 2019"* (interneta resurss: https://ec.europa.eu/taxation_customs/sites/taxation/files/customs_programme_progress_report_2019.pdf.pdf, resurss skatīts:12.04.2021.)

[81] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 6. punkts.

[82] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[83] Ministru kabineta 14.06.2016. noteikumu Nr.374 "Valsts informācijas sistēmu savietotāja noteikumi" 41. un 42. punkts.

[84] [IP]

[85] [IP]

[86] [IP]

[87] [IP]

[88] [IP]

[89] [IP]

[90] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts, 13. punkts, 15.1. apakšpunkts.

[91] Portāla viss.gov.lv sadaļa "VISS koplietošanas komponentes" (interneta resurss: https://viss.gov.lv/lv; interneta resurss skatīts: 01.11.2021.), Valsts reģionālās attīstības aģentūras 26.03.2019. iekšējie noteikumi Nr.1-2/19/6 "Valsts informācijas sistēmu savietotāja infrastruktūras pakalpojumu lietošanas noteikumi".

[92] Revidenta aplēse: kopējais stundu skaits 2021.gadā = 8760 stundas, no tām pieejamība jānodrošina darbdienās no plkst. 8.30 līdz 17.00 = 2121 stundas (99% no 2142 stundām), brīvdienās un svētku dienās = 6419 stundas (97% no 6618). Vidējā nodrošināmā portāla Latvija.lv pieejamība = ((2121 stundas + 6419 stundas)/8760 stundas) * 100% = 97,49 %.

[93] Revidenta aplēse: Vienas stundas administratīvā sloga izmaksas portālam Latvija.lv * četras stundas mēnesī = 16 tūkst. *euro/h* * 4 h = 64 tūkst. *euro*

[94] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.

[95] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.1., 8.4., 8.5., 27.2. apakšpunkti.

[96] Labā prakse – COBIT, ITIL.

[97] Priekšnoteikumi ietverti labās prakses *COBIT 4.1.* sadaļās "*DS5 Ensure Systems Security*", *"PO9.1 IT Risk Management Framework", "PO9.5 Risk Response", "IT Continuity Framework", "PO2.3 Data Classification Scheme"*, labās prakses *ITIL* sadaļās *"4.6.4.1 Security framework", "5.10 IT SERVICE CONTINUITY MANAGEMENT", "5.11 INFORMATION SECURITY MANAGEMENT"*, Ministru kabineta 28.07.2015. noteikumos Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".

[98] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 15.17. apakšpunkts.

[99] Priekšnoteikumi ietverti labās prakses *COBIT 4.1.* sadaļās "*DS5 Ensure Systems Security*", *"PO9.1 IT Risk Management Framework", "PO9.5 Risk Response", "IT Continuity Framework", "PO2.3 Data Classification*

Scheme", labās prakses *ITIL* sadaļās *"4.6.4.1 Security framework", "5.10 IT SERVICE CONTINUITY MANAGEMENT", "5.11 INFORMATION SECURITY MANAGEMENT".*

[100] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 6., 7., 10., 11. punkti,, 8.1., 8.4., 8.5, 13.1.–13.5., 27.1.–27.3., 29., 30.1.–30.5., 33.1.–33.4. apakšpunkti.

[101] LVRTC sniegtie pakalpojumi iestādēm (interneta vietne: https://www.lvrtc.lv/lvdc/; resurss apskatīts: 03.02.2021.).

[102] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 20.punkts.

[103] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[104] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 8. punkts.

[105] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 8. punkts.

[106] Ministru kabineta 19.06.2012. noteikumi Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības", Ministru kabineta 28.07.2015. noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".

[107] Ministru kabineta 04.07.2017. noteikumu Nr.402 "Valsts pārvaldes e-pakalpojumu noteikumi" 9.7. apakšpunkts.

[108] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.6. apakšpunkts.

[109] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 10. punkts.

[110] Labā prakse – COBIT 4.1. sadaļa "*DS4.5 Testing of the IT Continuity Plan*".

[111] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 20.punkts ar apakšpunktiem, 15.17. apakšpunkts.

[112] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 20.punkts, 33.4. apakšpunkts.

[113] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 15.17. apakšpunkts.

[114] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 25.4. apakšpunkts.

[115] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[116] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 33.4. apakšpunkts.

[117] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 25.4. apakšpunkts.

[118] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.6. apakšpunkts.

[119] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.4. apakšpunkts.

[120] "Latvijas Nacionālais attīstības plāns 2021.–2027.gadam" (apstiprināts ar Latvijas Republikas Saeimas 2020.gada 2.jūlija lēmumu Nr.418/Lm13), "Digitālās transformācijas pamatnostādnes 2021.–2027.gadam" (atbalstītas ar Ministru kabinetaā 07.07.2021. rīkojumu Nr.490), informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022.gadam" (apstiprināts Ministru kabinetā 2019.gada 17.septembrī, protokols Nr.42, 43.§).

[121] Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022.gadam" (apstiprināts Ministru kabinetā 2019.gada 17.septembrī, protokols Nr.42, 43.§).

[122] "Latvijas Nacionālais attīstības plāns 2021.–2027.gadam" rīcības virziens "Tehnoloģiskā vide un pakalpojumi" (apstiprināts ar Latvijas Republikas Saeimas 2020.gada 2.jūlija lēmumu Nr.418/Lm13).

[123] "Digitālās transformācijas pamatnostādnes 2021.–2027.gadam" (atbalstītas ar Ministru kabinetaā 07.07.2021. rīkojumu Nr.490) attīstības joma "Digitālā drošība".

[124] Starpposma novērtējums noteikts 2024. gada 31. maijā (Ministru kabineta 07.07.2021. rīkojuma Nr.490 "Par Digitālās transformācijas pamatnostādnēm 2021.-2027. gadam" 4. punkts.

[125] 2019.gada Valsts kontroles lietderības revīzijas "Vai valsts pārvaldē tiek noteikta vienota IKT infrastruktūras pārvaldība, lai nodrošinātu tās efektīvu izmantošanu?" ziņojuma 38.–39.lpp.
[126] Valsts informācijas sistēmu likuma 1. panta divpadsmitā daļa.
[127] Ministru kabineta 05.11.2019. noteikumu Nr.523 "Valsts informācijas resursu, sistēmu un sadarbspējas informācijas sistēmas noteikumi" 4. punkts.
[128] Ministru kabineta 19.03.2011. noteikumu Nr.233 "Vides aizsardzības un reģionālās attīstības ministrijas nolikums" 5.7.5., 5.7.7., 5.7.8. apakšpunkti.
[129] Ministru kabineta 05.11.2019. noteikumu Nr.523 "Valsts informācijas resursu, sistēmu un sadarbspējas informācijas sistēmas noteikumi" 31. punkts.
[130] VIRSIS dati (dati pieejami: https://data.gov.lv/dati/lv/dataset/valsts-informacijas-un-kumunikaciju-tehnologiju-resursi-un-ikt-starpiestazu-pakalpojumi/resource/dd6088a4-5c6c-4805-b6a9-ca22ff6ede8b). Dati analizēti 02.01.2022.
[131] VIRSIS reģistru bloku un lauku apraksti v1.2-12 (apraksts pieejams: https://viss.gov.lv/lv/Informacijai/Dokumentacija/Vadlinijas/VIRSIS, interneta resurss skatīts: 23.03.2022.)
[132] Ministru kabineta 05.11.2019. noteikumu Nr.523 "Valsts informācijas resursu, sistēmu un sadarbspējas informācijas sistēmas noteikumi" 16.1.1.2.2. un 16.2.1.2.2. apakšpunkti.
[133] VIRSIS reģistru bloku un lauku apraksti v1.2-12 (apraksts pieejams: https://viss.gov.lv/lv/Informacijai/Dokumentacija/Vadlinijas/VIRSIS, interneta resurss skatīts: 23.03.2022.)
[134] Ministru kabineta 05.11.2019. noteikumu Nr.523 "Valsts informācijas resursu, sistēmu un sadarbspējas informācijas sistēmas noteikumi" 16. punkts.
[135] "Valsts civilās aizsardzības plāna" (apstiprināts ar Ministru kabineta 26.08.2020. rīkojumu Nr.476 "Par Valsts civilās aizsardzības plānu") 29. pielikumā minētās IS.
[136] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 5.1. apakšpunkts.
[137] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.
[138] MK 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 6. punkts.
[139] VIRSIS dati (dati pieejami: https://data.gov.lv/dati/lv/dataset/valsts-informacijas-un-kumunikaciju-tehnologiju-resursi-un-ikt-starpiestazu-pakalpojumi/resource/dd6088a4-5c6c-4805-b6a9-ca22ff6ede8b); datu analīze veikta: 04.01.2022.
[140] Kritērijs "IS drošības politika" pēc MK442 prasībām attiecas uz visām IS, revīzijā pēc šī kritērija tika vērtētas visas IS.
[141] Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 13.1.–13.5. apakšpunkti.
[142] Kritērijs "Sistēmas drošības risku izvērtējums" pēc MK442 prasībām attiecas tikai uz paaugstinātas drošības IS, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.
[143] Prasību nosaka Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 30. punkts.
[144] Kritērijs "IS drošības riska pārvaldības plāns" pēc MK442 prasībām attiecas tikai uz paaugstinātas drošības IS, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.
[145] Prasību nosaka Ministru kabineta 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 30. punkts.
[146] Kritērijs "IS darbības atjaunošanas plāns" pēc MK442 prasībām attiecas tikai uz paaugstinātas drošības IS, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.
[147] Prasību nosaka MK 28.07.2015. noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 33. punkts.
[148] Kritērijs pēc MK421 prasībām attiecas tikai uz integrētājām valsts informācijas sistēmām un savietotāju, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.
[149] Kritērijs "UPS iekārtas ir pārbaudītas, vai spēj nodrošināt strāvas padevi līdz 30 min" pēc MK421 prasībām attiecas tikai uz integrētājām valsts informācijas sistēmām un savietotāju, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.
[150] Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 9.3. apakšpunkts.

[151] Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) mājas lapa – Informācija par CERT.LV sensoru tīklu (Agrīnās brīdināšanas sistēmu) (interneta resurss: https://cert.lv/lv/pamatpakalpojumu-un-digitalo-pakalpojumu-sniedzejiem, resurss skatīts 12.02.2021.)

[152] [IP]

[153] [IP]

[154] Kritērijs "Rezerves kopiju veidošanas un atjaunošanas kārtība" pēc MK442 prasībām attiecas tikai uz paaugstinātas drošības IS, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.

[155] Kritērijs "Rezerves kopiju glabāšana" pēc MK421 prasībām attiecas tikai uz integrētājām valsts informācijas sistēmām un savietotāju, tomēr revīzijā pēc šī kritērija tika vērtētas visas IS.

[156] Prasību nosaka Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.1., 10.2. un 10.6. apakšpunkti.

[157] Prasību nosaka Ministru kabineta 19.06.2012. noteikumu Nr.421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" 10.4. apakšpunkts.

[158] CERT.LV 2021. gada 4. ceturkšņa "Publiskais pārskats par CERT.LV uzdevumu izpildi" (interneta resurss: https://cert.lv/uploads/parskati/cert-ceturksna-C4-atskaite-2021-LV.pdf; resurss skatīts 01.06.2022.)