



ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem

VPP-COVID-2020/1-0009

***Izvērtējums par jaunu informācijas un
komunikācijas tehnoloģiju risinājumu
izmantošanas potenciālu uzņēmējdarbības
sektorā krīzes/ pēckrīzes apstākļos***

Autori: R. Pirta-Dreimane, I. Auliciema, M. Stučka, I. Reinholde

Versija, datums: 1.0. 30.11.2020.

Labojumu vēsture

Versija	Apraksts	Autors
1.0.	Dokumenta sākotnējā versija	R.Pīrta-Dreimane I. Auliciema M. Stučka I. Reinholde

Satura rādītājs

Ievads	6
1. Pētījuma metodika	7
1.1. Juridiskais un organizacionālais līmenis	8
1.2. Semantiskais līmenis	9
1.3. Tehniskais līmenis	10
2. Pētāmās problēmas teorētiskais skaidrojums	10
2.1. Krīzes situācijas veidošanās un attīstība	10
2.2. Krīzes pārvaldības principi	13
2.3. Risku analīzes pieeja	15
3. Esošā situācija rīcībpolitikas jomā	18
3.1. Attālinātais darbs	18
3.1.1. Normālā situācijā	18
3.1.2. Ārkārtējās situācijas laikā	19
3.1.3. Atkopšanās situācijā	20
3.1.4. Jaunajā normālajā situācijā	22
3.2. Digitālā transformācija	23
3.2.1. Normālajā situācijā	23
3.2.2. Ārkārtējā situācijas laikā	25
3.2.3. Atkopšanās situācijā un jaunajā normālajā situācijā	25
4. Jaunu IKT izmantošanas potenciāls uzņēmējdarbībā	27
4.1. Uzņēmumu digitālā brieduma līmenis	27
4.2. Aktuālās digitalizācijas tendences uzņēmējdarbībā	28
4.2.1. Tendencu kopsavilkums	28
4.2.2. Tendencu salīdzinošā analīze	36
4.3. Digitalizāciju kavējošie un veicinošie faktori	37
4.3.1. Kavējošie faktori	37
4.3.2. Veicinošie faktori	37
5. Servisu drošības un noturības nodrošināšanas paņēmieni	38
6. Priekšlikumi	39
6.1. Priekšlikumi uzņēmējiem	39
6.1.1. Biznesa nepārtrauktības nodrošināšana	39
6.1.1.1. Kritisko spēju orientēta biznesa nepārtrauktības plānošana	39
6.1.1.2. Digitālā dvīņa izmantošana ārkārtas situāciju un pakalpojumu dinamiskai simulēšanai un monitoringam	40
6.1.1.3. Risku analīzē saknota procesu un pakalpojumu pielāgojumu plānošana	41

6.1.1.4.	Informācijas drošība kā stratēģiskā digitālā spēja	41
6.1.1.5.	Spējo paradigmu izmantošana pārmaiņu vadībā	41
6.1.2.	Digitāli iespējots drošs attālinātais darbs un attālināta pakalpojumu sniegšana	41
6.1.2.1.	Digitālā brieduma līmenī sakņota tehnoloģiju izvēle	41
6.1.2.2.	IKT kā pakalpojuma izmantošana	44
6.1.2.3.	Komandu kopdarbības veicināšana attālinātajā darbā	45
6.1.2.4.	Droši pamatservisi jeb droša tīkla pārvaldība	45
6.1.3.	Efektīva un atbildīga resursu pārvaldība	46
6.1.3.1.	Ārkārtējās situācijas pārvarēšanas zināšanu koplietošana	46
6.1.3.2.	Efektīvas un drošas komunikācijas veicināšana un pārvaldība	46
6.1.3.3.	Darbinieku motivācijas līmeņa monitorings	48
6.1.3.4.	Digitālo ekosistēmu izveide resursu optimizācijai	48
6.1.3.5.	Digitālā ētika kā uzņēmuma politikas sastāvdaļa	48
6.1.3.6.	Digitālo prasmju un digitālo spēju stiprināšana	49
6.2.	Priekšlikumi valsts atbalstam un intervencei	49
6.1.1.	Risku analīzē balstīta krīžu pārvaldība	50
6.1.1.1.	Kontekstuālo risku analīzes/ietekmes izvērtēšanas ieviešana	50
6.1.1.2.	Kontekstuālos riskos balstīta krīžu pārvaldība	51
6.1.2.	Jaunās darba formas atbalstoša darba un komunikācijas kultūra	52
6.1.2.1.	Skaidri un līdzsvaroti attālinātā darba “spēles noteikumi”	52
6.1.2.2.	Informācijas aizsardzība un digitālā ētika kā pienākums uzņēmējiem	52
6.1.3.	Uzņēmējdarbības digitalizācijas veicināšana	53
6.1.3.1.	Motivējošie faktori digitālo tehnoloģiju izmantošanas veicināšanai	53
6.1.3.2.	Pētniecības un izstrādes (R&D) veicināšana	54
6.1.3.3.	Inovāciju koplietošanas ekosistēmas attīstība	54
6.1.3.4.	Uzņēmumu digitālo prasmju un digitālo spēju stiprināšana	55
	Literatūra	56
	1.pielikums “Droša un noturīga servisa piemērs”	61
	Droši pamatservisi	61
	Spējas modelis	61
	2.pielikums “Rekomendācijas komandu kopdarbības rīkiem”	64
	3.pielikums “Šablona piemērs”	68
	4.pielikums “Digitālā dvīņa piemērs”	69
	5.pielikums “Tehnoloģiju izmantošanas rekomendācijas”	70

Kopsavilkums

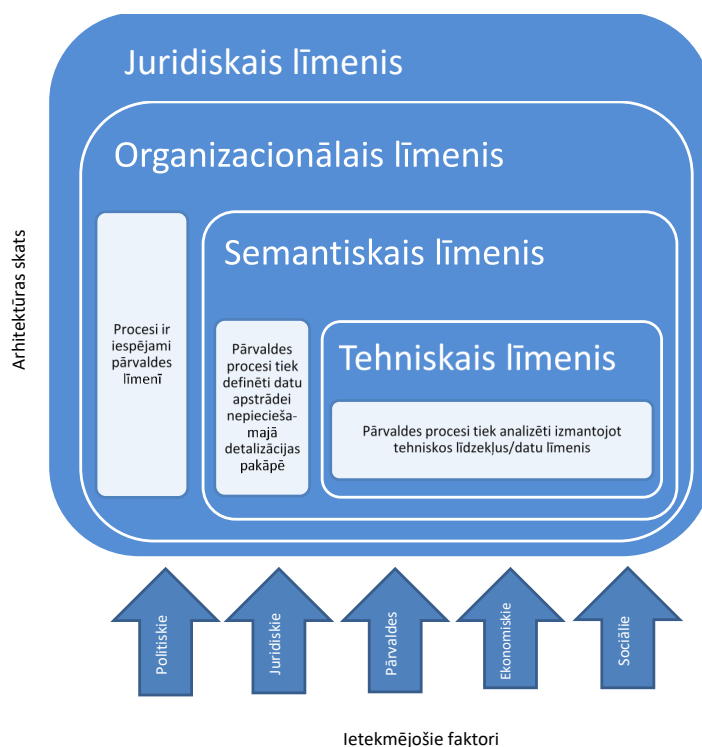
Projekta „ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem” (VPP-COVID-2020/1-0009) (turpmāk tekstā – Projekts) mērķis ir izstrādāt metodi un tehnoloģiskos risinājumus digitālo pakalpojumu dinamiskai pielāgošanai un drošības nodrošināšanai COVID-19 gadījumā un līdzīgās krīzes situācijās.

Dokumentā „Izvērtējums par jaunu informācijas un komunikācijas tehnoloģiju risinājumu izmantošanas potenciālu uzņēmējdarbības sektorā krīzes/ pēckrīzes apstākļos” (turpmāk tekstā – Izvērtējums) sniegta rekomendācijas par:

- dažādu informācijas un komunikācijas tehnoloģiju risinājumu izmantošanas potenciālu, tostarp vecinošiem un kavējošiem regulatīviem un uzņēmējdarbības vides apstākļiem uzņēmējdarbības sektorā krīzes/ pēckrīzes apstākļos;
- būtiskākajām informācijas un komunikācijas tehnoloģijām un to pielietojumiem, kas nodrošina uzņēmējdarbības procesu nepārtrauktību, tostarp nepieciešamais valsts atbalsts vai intervence tehnoloģiju plašākai izmantošanai uzņēmējdarbībā.

Izvērtējums aptver plašu jautājumu loku, sākot ar rīcībpolitiku izstrādi un beidzot ar tehnoloģisku risinājumu modelēšanu uzņēmējdarbības vajadzībām, tādēļ Izvērtējuma un rekomendāciju sagatavošanā pētāmie jautājumi nosacīti iedalāmi vairākos līmeņos jeb arhitektūras skatos (European Commission, 2020) (Ilustrācija 1):

1. Juridiskais līmenis, kas definē juridisko ietvaru (tiek apskatīts kopā ar organizatorisko līmeni);
2. Organizacionālais līmenis, kas paredzēts rīcībpolitiku plānošanai, normatīvo aktu izstrādei, kā arī uzņēmēju, nodarbināto, publiskās pārvaldes institūciju un iedzīvotāju vajadzību izpētei;
3. Semantiskais līmenis, kurā tiek veikta organizacionālajā līmenī izmantotās terminoloģijas salāgošana ar tehnoloģiju izpētē un modelēšanā izmantoto terminoloģiju un paaugstināta apskatāmo procesu detalizācijas pakāpe;
4. Tehniskais līmenis, kur pētītas tehnoloģiju izmantošanas iespējas drošu un nepārtrauktu servisu nodrošināšanai.

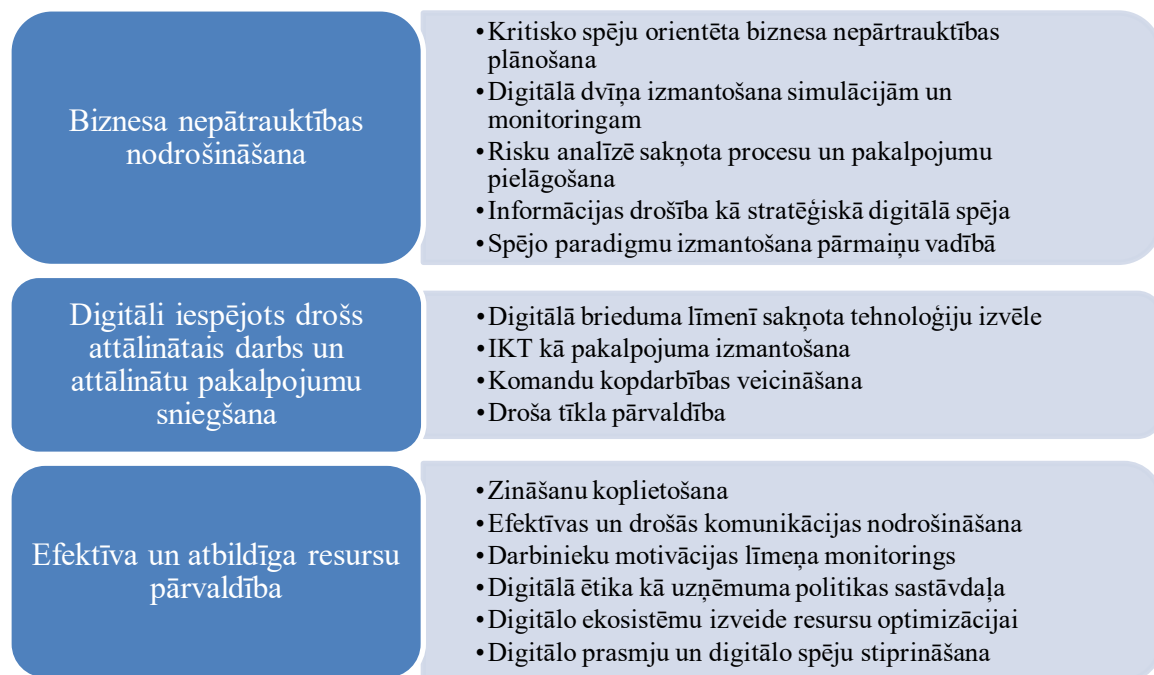


Ilustrācija 1 Pētījuma pieeja

Izvērtējuma rezultātā sniegti priekšlikumi par būtiskākajiem veicamajiem organizatoriskajiem pasākumiem drošu un noturīgu servisu nodrošināšanai, tehnoloģijām un to pielietojumiem, kas nodrošina uzņēmējdarbības procesu nepārtrauktību, kā arī rekomendācijas nepieciešamajam valsts atbalstam vai valsts intervencei tehnoloģiju plašākai izmantošanai uzņēmējdarbībā.

Priekšlikumi uzņēmējiem aptver trīs galvenos virzienus (Ilustrācija 2):

1. Biznesa nepārtrauktības nodrošināšana – priekšlikumi preventīvajiem un uzraudzības pasākumiem, kas veicami biznesa nepārtrauktības nodrošināšanai ārkārtas situācijās;
2. Digitāli iespējots drošs un nepārtraukts darbs – priekšlikumi tehnoloģiju izmantošanai attālinātā darba organizācijai ārkārtas situācijā (tehnoloģiju un rīku izmantošana, digitālas darba vietas, izkliegtu komandu kopdarbība u.c.);
3. Efektīva un atbildīga resursu pārvaldība – priekšlikumi uzņēmumu resursu efektīvai pārvaldībai ārkārtas situācijā (zināšanas, cilvēkresursi u.c.).



Ilustrācija 2 Priekšlikumi uzņēmējiem drošu un noturīgu servisu nodrošināšanai

Priekšlikumi valsts atbalstam un intravencei aptver trīs galvenos virzienus (Ilustrācija 3):

1. Risku analīzē balstīta krīžu pārvaldība – priekšlikumi kontekstuālo risku analīzei un riskos balstītai krīžu pārvaldībai, plānojot uzņēmējdarbības atbalstu un valsts intravenci;
2. Jaunās darba formas atbalstoša darba un komunikācijas kultūra – priekšlikumi noteikumu un vadlīniju izveidei valsts līmenī;
3. Uzņēmumu digitalizācijas veicināšana – priekšlikumi valstiski veicamajiem pasākumiem uzņēmumu digitalizācijas veicināšanai.

Risku analīzē balstīta krīžu pārvaldība	<ul style="list-style-type: none">• Kontekstuālo risku analīzes/ietekmes novērtēšanas ieviešana• Kontekstuālajos riskos balstīta krīžu pārvaldība
Jaunās darba formas atbalstoša darba un komunikācijas kultūra	<ul style="list-style-type: none">• Skaidri un līdzsvaroti attālinātā darba "spēles noteikumi"• Informācijas aizsardzība un digitālā ētika kā pienākums uzņēmējiem
Uzņēmējdarbības digitalizācijas veicināšana	<ul style="list-style-type: none">• Ekonomisks pamats digitālo tehnoloģiju izmantošanas veicināšanai• Digitālās ētikas vadlīniju izstrāde• Pētniecības un izstrādes (R&D) veicināšana• Inovāciju koplietošanas ekosistēmu attīstība• Uzņēmumu digitālo prasmju un digitālo spēju stiprināšanas atbalsts

Ilustrācija 3 Priekšlikumi valsts intravencei un atbalstam

Termini un saīsinājumi

Termins	Skaidrojums
ARTSS, Projekts	Projekts "ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem" (VPP-COVID-2020/1-0009)
Ārkārtējā situācija	Īpašs tiesiskais režīms, kura laikā Ministru kabinetam ir tiesības likumā noteiktajā kārtībā un apjomā ierobežot valsts pārvaldes un pašvaldību institūciju, fizisko un juridisko personu tiesības un brīvības, kā arī uzlikt tām papildu pienākumus.
Biznesa serviss	Šī dokumenta kontekstā – pasažieru pārvadājumu pakalpojumi
Digitalizācija	Digitālo tehnoloģiju izmantošana jaunu produktu, pakalpojumu un pievienotās vērtības radīšanai
Digitālais briedums	Mērs uzņēmuma digitālo spēju mērīšanai
Digitālais dvīnis <i>Digital twin</i>	Reālā servisa nodrošināšanas tīkla attēlojums virtuālajā videi kontrolei un analīzei
Drošības aspekts	Mērķa specializācija, kas attēlo drošības mērķus
Ekosistēma <i>Ecosystem</i>	Visu drošu un noturīgu servisu nodrošināšanu ietekmējamo iesaistīto pušu kopums
IKT	Informācijas un komunikācijas tehnoloģija
Izvērtējums	ARTSS projekta ietvaros veikts izvērtējums par jaunu informācijas un komunikācijas tehnoloģiju risinājumu izmantošanas potenciālu uzņēmējdarbības sektorā krīzes/ pēckrīzes apstākļos
Katastrofa	Notikums, kas izraisījis cilvēku upurus un apdraud cilvēku dzīvību vai veselību, nodarījis kaitējumu vai radījis apdraudējumu cilvēkiem, videi vai īpašumam, kā arī radījis vai rada būtiskus materiālos un finansiālos zaudējumus un pārsniedz atbildīgo valsts un pašvaldības institūciju ikdienas spējas novērst notikuma postošos apstākļus
Konteksta elements <i>Context Element</i>	Uz datiem balstīta informācija, kas raksturo situāciju, kurā sistēma darbojas.
KPI	Mērs mērķa sasniegšanas mērīšanai
Krīzes situācija	Notikums, kas, ja tam ļauj saasināties, var pārtraukt organizācijas ikdienas darbu un apdraud tās reputāciju, kā arī grauj pamatbūtību (Siliņa, 2018)
Mācīšanās modulis	Nodrošina apmācību par servisa drošu izmantošanu
Mērāmu datu vienība <i>Measurable property</i>	Spējas nodrošināšanas un servisa darbības vides mērījumi
Mērķis <i>Goal</i>	Dažādu lietu un apstākļu vēlamais stāvoklis, kuru nepieciešams sasniegt
Pamatserviss	IKT servisi, kas nodrošina citu digitālo pakalpojumu darbību un drošu tīklošanu (šī dokumenta kontekstā – tīkla pakalpojumi)
Pielāgojums <i>Adjustment</i>	Algoritmiska rekomendācija spējas pielāgošanai atbilstoši konteksta situācijai
Serviss	Komponente, kas, nodrošina noteiktu funkcionalitāti atbildot uz partnera pieprasījumu
Spēja <i>Capability</i>	Varēšana un kapacitāte sasniegt organizācijas mērķus mainīgos kontekstuālos apstākļos

Termins	Skaidrojums
Šablons	Strukturētas, atkāroti izmantojamas zināšanas par drošu un noturīgu servisu izstrādi un darbināšanu
Tīkls	Servisa nodrošinātāju kopumus

Ievads

Projekta „ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem” (VPP-COVID-2020/1-0009) (turpmāk tekstā – Projekts) mērķis ir izstrādāt metodi un tehnoloģiskos risinājumus digitālo pakalpojumu dinamiskai pielāgošanai un drošības nodrošināšanai COVID-19 gadījumā un līdzīgās krīzes situācijās.

Atbilstoši 10.07.2020.līgumam nr.6-1/7, kas noslēgts starp Latvijas zinātnes padomi un Rīgas Tehnisko universitāti (turpmāk tekstā – Līgums), projekta realizācija notiek un nodevumi tiek sagatavoti atbilstoši projekta pieteikumam (Līguma 1.pielikums), rekomendācijām projekta īstenošanai (projekta 8.pielikums) un papildus projekta rezultātu sarakstam (Līguma 9.pielikums).

Dokuments „Izvērtējums par jaunu informācijas un komunikācijas tehnoloģiju risinājumu izmantošanas potenciālu uzņēmējdarbības sektorā krīzes/ pēckrīzes apstākļos” (turpmāk tekstā – Izvērtējums) tiek sagatavots atbilstoši projekta pieteikumam, kas paredz sniegt konkrētas rekomendācijas par:

- optimālām jauna formāta digitalizētām darba vietām,
- jaunām individuālā un kolektīvā darba pieejām,
- sabiedriskā sektora darbu digitālajā formātā

Atbilstoši līguma 9.pielikumam, tiek veikts izvērtējums un sniegtas rekomendācijas par:

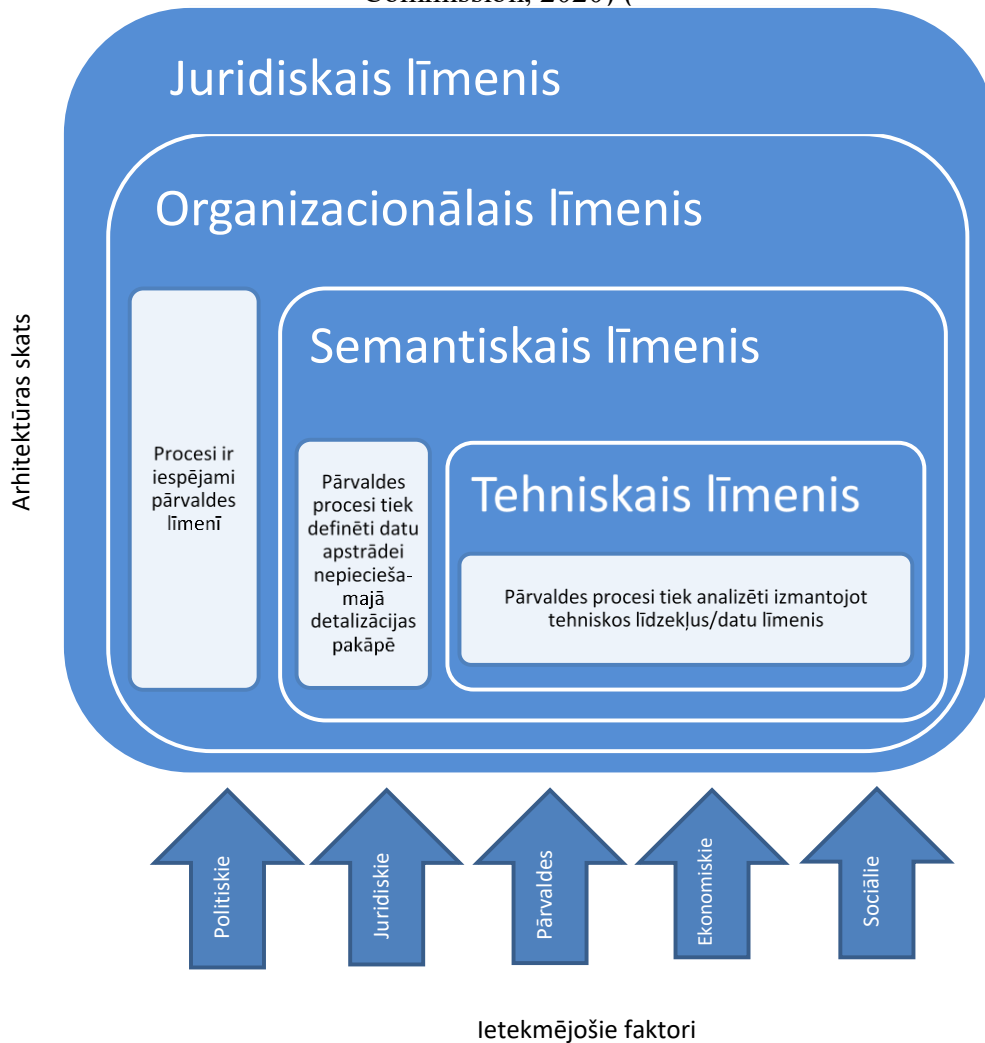
- dažādu informācijas un komunikācijas tehnoloģiju risinājumu izmantošanas potenciālu, tostarp vecinošiem un kavējošiem regulatīviem un uzņēmējdarbības vides apstākļiem uzņēmējdarbības sektorā krīzes/ pēckrīzes apstākļos, piemēram, (a) komunikācijas uzņēmumu starpā (B2B), starp uzņēmumiem un patērētājiem (B2C), starp uzņēmumiem un publisko sektoru (B2G) jomā; (b) digitālo risinājumu un tehnoloģiju izmantošana pakalpojumu nodrošināšanas jomā un ražošanas procesos.
- būtiskākajām informācijas un komunikācijas tehnoloģijām un to pielietojumiem, kas nodrošina uzņēmējdarbības procesu nepārtrauktību, tostarp sniegt priekšlikumus nepieciešamajam valsts atbalstam vai valsts intervencei informācijas un komunikācijas tehnoloģiju plašākai izmantošanai uzņēmējdarbībā.

Rekomendāciju pamatā ir Projektā izstrādātā ARTSS metode, kā arī secinājumi no literatūras analīzes (IKT izmantošanas tendences krīzes situācijās, risku pārvaldības modeļi u.c.). Metode paredz strukturētu pakalpojuma mērķu, izpildes rādītāju, konteksta (jeb izpildes vides mērījumu) un drošības un noturības pielāgojumu attēlošanu un izmantošanu servisa konfigurēšanā tā izstrādes un izpildes laikā.

Izvērtējums iekļauj sešas nodaļas. Pirmajā nodaļā aprakstīta pētījuma metodika dažādos līmeņos jeb arhitektūras skatos – juridiskais, organizacionālais, semantiskais un tehniskais. Otrajā nodaļā izklāstīta pētāmā problēma, analizējot krīzes situācijas veidošanās situācijas, krīzes pārvaldības principus un piedāvājot risku analīzes pieeju. Trešajā nodaļā sniegts esošo rīcībpolitiku apskats, izdalot divas jomas – attālināts darbs un digitālā transformācija. Ceturtajā nodaļā izvērtētas jaunu IKT izmantošanas iespējas, analizējot aktuālās pasaules tendences un salīdzinot to piemērošanu dažādās situācijās (normālā situācija, krīzes situācija u.c.). Piektajā nodaļā piedāvāti servisu drošības un noturības paņēmieni. Izvērtējums noslēdzas ar priekšlikumiem uzņēmējiem tehnoloģiju izmantošanai drošu un noturīgu servisu nodrošināšanai un priekšlikumiem valsts intravencei un atbalstam tehnoloģiju izmantošanas veicināšanai.

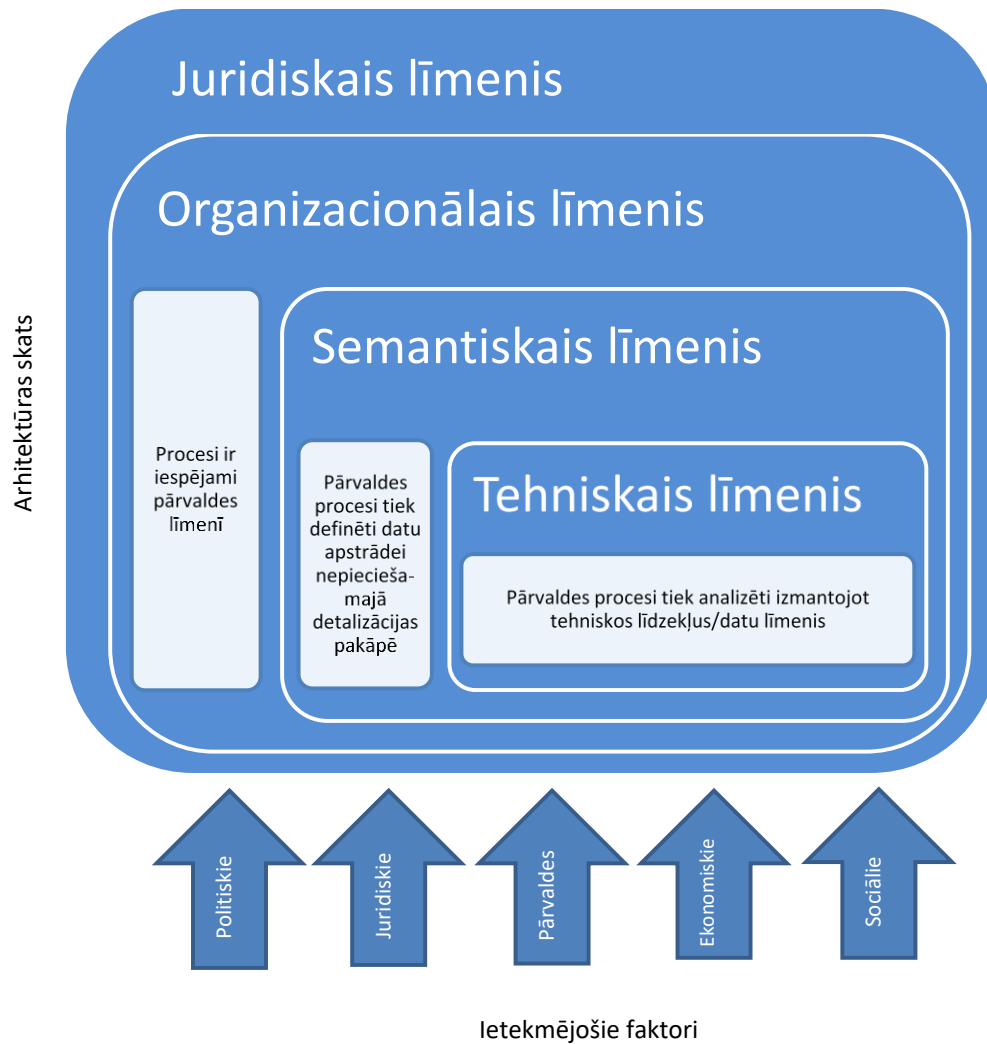
1. Pētījuma metodika

Projekts aptver plašu jautājumu loku, sākot ar rīcībpolitiku izstrādi un beidzot ar tehnoloģisku risinājumu modelēšanu uzņēmējdarbības vajadzībām, tādēļ Izvērtējuma un rekomendāciju sagatavošanā pētāmie jautājumi nosacīti iedalāmi šādos līmeņos (European Commission, 2020) (



Ilustrācija 4):

1. Juridiskais līmenis, kas definē juridisko ietvaru (tiek apskatīts kopā ar organizatorisko līmeni);
2. Organizacionālais līmenis, kas paredzēts rīcībpolitiku plānošanai, normatīvo aktu izstrādei, kā arī uzņēmēju, nodarbināto, publiskās pārvaldes institūciju un iedzīvotāju vajadzību izpētei;
3. Semantiskais līmenis, kurā tiek veikta organizacionālajā līmenī izmantotās terminoloģijas salāgošana ar tehnoloģiju izpētē un modelēšanā izmantoto terminoloģiju un paaugstināta apskatāmo procesu detalizācijas pakāpe;
4. Tehniskais līmenis, kur pētītas tehnoloģiju izmantošanas iespējas drošu un nepārtrauktu servisu nodrošināšanai.

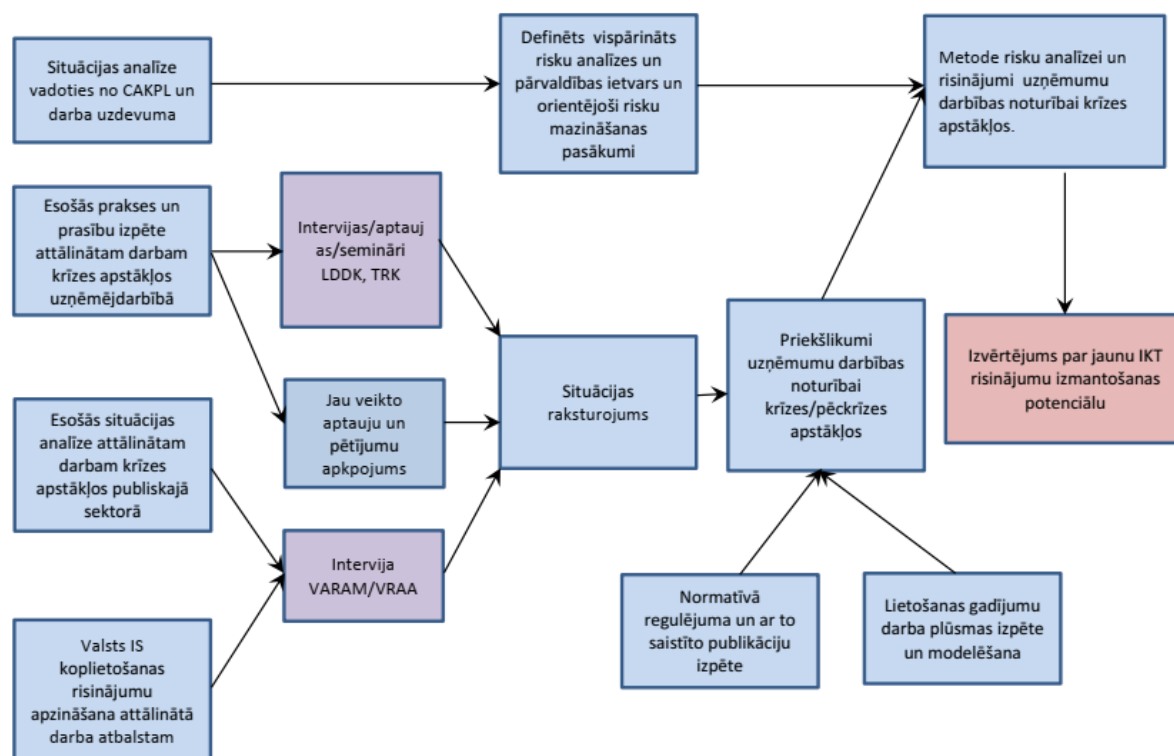


Ilustrācija 4 Pētījuma pieeja

1.1. Juridiskais un organizacionālais līmenis

Organizacionālā līmeņa izvērtējums tiek uzsākts ar atskaites punktu definēšanu, kas parāda normalitātes, krīzes, pēckrīzes atkopšanās posmu laiku un pazīmes, kā arī prasības biznesa, publiskās pārvaldes, kā arī mājsaimniecību (biznesā nodarbināto un klientu statusā) funkcionēšanai.

Šajā posmā izvērtējumā tiek apzinātas risku pārvaldības metodes, kā arī veikta politikas plānošanas dokumentu un normatīvo aktu analīze jomās, kas attiecas uz digitālās transformācijas jautājumiem un attālināto darbu.



Ilustrācija 5 Izvērtējuma metodika organizacionālajā līmenī

Ievērojot, ka strādājot ārkārtas situācijas apstākļos jau ir uzkrāta pieredze attālinātā darba organizēšanai un pakalpojumu sniegšanai, tiks veikta esošās prakses un prasību izpēte attālinātam darbam krīzes apstākļos uzņēmējdarbībā un publiskajā sektorā. Tāpat tiks apzināts valsts informācijas sistēmu koplietošanas risinājumu klāsts, lai izvērtētu pilnvērtīgas tālrunu izmantošanas iespējas.

Ņemot vērā, ka paralēli notiek vairāku projektu izstrāde, kuros viena no aktivitātēm ir dažādu attālinātā darba sistēmu lietotāju (uzņēmēju, darbinieku, sabiedrisko organizāciju) aptaujas un intervijas, kuru jautājumi lielā mērā pārklājas, šī pētījuma pamatā tiks izmantoti gan jau publicētie citu pētījumu dati, tos nepieciešamības gadījumā papildinot ar ieinteresēto institūciju pārstāvju intervijām, kā arī tematisku semināru materiāliem.

Darba gaitā tika intervēti šādu organizāciju pārstāvji:

- Ekonomikas ministrija;
- Vides un Reģionālās attīstības ministrija;
- Tirdzniecības un rūpniecības kamera.

Pētījumā izmantota Latvijas darba devēju konfederācijas ekspertu, kā arī Latvijas Brīvo arodbiedrību savienības ekspertu sniegtā informācija seminārā „Jaunā darba vide”, kas notika 2020. gada 12. novembrī.

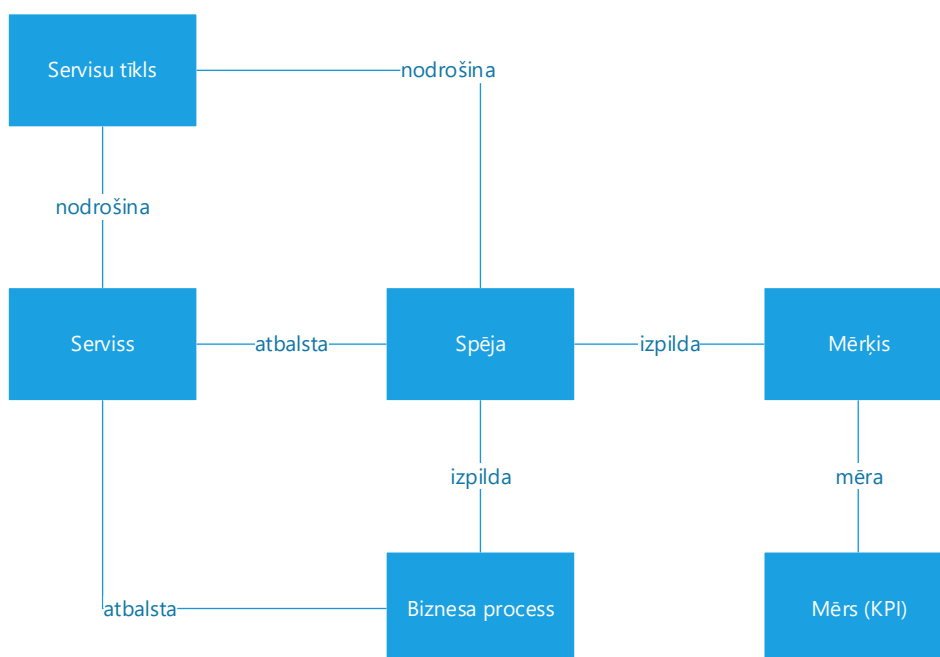
Papildus tam, tiks veikts plašāks jau veikto pētījumu apkopojums, kā arī analīze jautājumos, kas attiecas uz attālināto darbu.

Balstoties uz apkopoto informāciju un lietošanas gadījumu analīzi, izmantojot risku pārvaldības metodoloģiju, tiks izstrādātas rekomendācijas optimālu jauna formāta digitalizētu darba vietu izveidei, jaunu individuālā un kolektīvā darba pieeju ieviešanai uzņēmējiem, to darbiniekiem, klientiem un publiskajam sektoram.

1.2. Semantiskais līmenis

Semantiskajā līmenī tiek savietoti organizatoriskā un tehniskā līmenī izmantotie jēdzieni, kas ir daļa no ARTSS metodes konceptu modeļa (Ilustrācija 6).

Organizacionālais jeb biznesa līmenis ar tehnoloģiju līmeni tiek sasaistīts, izmantojot spēju modeļus. Serviss nodrošina savstarpēji saistītu servisu sniedzēju tīkls. Spēja definē servisu tīkla un tā dalībnieku varēšanu un kapacitāti nodrošināt servisa noturību un drošību. Servisu tīklam ir vienoti mērķi, un tas apmainās ar kontekstuālo informāciju un zināšanām savstarpējās uzticēšanās ietvaros. Lai nodrošinātu drošus un noturīgus servissus, servisu tīklam ir jāpiemīt atbilstošām drošības un noturības spējām. Spēju nodrošināšanai tiek realizēti viens vai vairāki biznesa procesi un tiek izmantoti vairāki digitālie servisi. Servissus nodrošina no atsevišķiem mezgliem jeb servisu nodrošinātājiem sastāvošs servisu tīkls. Servisu nodrošinātāji veido drošu un noturīgu servisu ekosistēmu, kurā notiek pakāpeniska savstarpēji bagātinoša spēju attīstīšana, balstoties uz uzkrātajām zināšanām.



Ilustrācija 6 ARTSS konceptu modeļa fragments

1.3. Tehniskais līmenis

Tehniskā līmeņa izvērtējums tiek uzsākts ar uzņēmēju digitālā brieduma līmeņu definēšanu un Latvijas uzņēmumu digitālā brieduma līmeņa identificēšanu. Digitālā brieduma līmenis tiks noteikts, pamatojoties uz Latvijas informācijas un tehnoloģiju asociācijas (LIKTA) izveidoto risinājumu <https://www.gudralatvija.lv/>.

Nākamais solis ir uzņēmējdarbības digitalizācijas tendenču analīze. Tendencu analīzei dokumentā izmantoti šādi avoti:

- Zinātniskā un nozares literatūra (2015.-2020. gads);
- Pētniecības un inovācijas projektu apraksti Latvijā (Kompetences centru programma) un pasaulē (“Apvārsnis 2020” programma) (2016.-2020. gads);
- Stratēģiskie plānošanas dokumenti Latvijā (piemēram, VARAM dokumenti) un Eiropā (programma “Digitālā Eiropa” u.c.).
- Intervijas ar uzņēmēju pārstāvjiem.

Balstoties uz analīzes rezultātiem katram brieduma līmenim tiks izvirzītas tehnoloģiju izmantošanas rekomendācijas (5. pielikums).

Papildus uzņēmuma līmenī izmantotajām tehnoloģijām, apskatīti valsts jau piedāvātie koplietošanas risinājumi uzņēmējiem, analizētas neatbilstības un izvirzītas rekomendācijas jaunu risinājumu izveidei un attīstībai (6.1.3.3. nodaļa).

2. Pētāmās problēmas teorētiskais skaidrojums

2.1. Krīzes situācijas veidošanās un attīstība

Ārkārtas situācijas izsludināšana 2020. gada 12. martā ienesa būtiskas izmaiņas sabiedrības dzīvē kopumā, t.sk. noteica virkni ierobežojumu, kas sekojoši radīja virkni izaicinājumu publiskās pārvaldes institūcijām, uzņēmējiem un ikvienam indivīdam.

Ministru kabinets rīkojumu nr.103 "Par ārkārtas situācijas izsludināšanu" izdeva atsaucoties uz Pasaules veselības organizācijas 2020. gada 11. marta paziņojumu, ka Covid-19 ir sasniegusi pandēmijas apmērus un pamatojoties uz Civilās aizsardzības un katastrofu pārvaldīšanas likuma 4. panta pirmās daļas 1. punkta "e" apakšpunktu, likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" 5.panta pirmo daļu un 6.panta pirmās daļas 1. punktu un otro daļu, 7. panta 1. punktu un 8. pantu un Epidemioloģiskās drošības likuma 3. panta otro daļu.

Civilās aizsardzības un katastrofu pārvaldīšanas likuma (Turpmāk – CAKPL) 4. pants nosaka katastrofu veidus un mērogus. Atbilstoši šī panta pirmās daļas 1. punkta "e" apakšpunktam Covid-19 pandēmija ir klasificēta kā bioloģiskā katastrofa.

CAKPL 1. panta 2.punkts definē katastrofu kā notikumu, kas izraisījis cilvēku upurus un apdraud cilvēku dzīvību vai veselību, nodarījis kaitējumu vai radījis apdraudējumu cilvēkiem, videi vai īpašumam, kā arī radījis vai rada būtiskus materiālos un finansiālos zaudējumus un pārsniedz atbildīgo valsts un pašvaldības institūciju ikdienas spējas novērst notikuma postošos apstākļus.

Savukārt katastrofa CPKPL izpratnē ir notikums kas jau ir izraisījis sekas, kas pārsniedz atbildīgo valsts un pašvaldības institūciju ikdienas spējas novērst notikuma postošos apstākļus. Latvijas saslimstības rādītāji 2020. gada marta līdz septembra mēnešos liecina, ka šajā gadījumā katastrofa CAKPL izpratnē nav iestājusies, toties pastāv katastrofas draudi. CAKPL 1. panta 3.punkts definē katastrofas draudus kā situāciju, kad risku novērtējums, prognozes, informācija vai citi apstākļi pamatoti liecina par katastrofas iespējamību.

Likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" (turpmāk tekstā – LĀSIS) 4. pants definē ārkārtēju situāciju kā īpašu tiesisko režīmu, kura laikā Ministru kabinetam ir tiesības likumā noteiktā kārtībā un apjomā ierobežot valsts pārvaldes un pašvaldību institūciju, fizisko un juridisko personu tiesības un brīvības, kā arī uzlikt tām papildu pienākumus. Katastrofa un tās draudi, ja būtiski apdraudēta valsts, sabiedrības, vides, saimnieciskās darbības drošība vai cilvēku dzīvība var būt pamats ārkārtas situācijas izsludināšanai.

Papildus, Epidemioloģiskās drošības likuma (turpmāk - EDL) 3. panta otrā daļa piešķir Ministru kabinetam tiesības noteikt epidemioloģiskās drošības pasākumus atsevišķu infekcijas slimību izplatības ierobežošanai. Epidemioloģiskā drošība EDL izpratnē ietver:

1. pasākumus veselīgas vides nodrošināšanai;
2. infekcijas slimību epidemioloģisko uzraudzību, tajā skaitā:

- a) infekcijas slimību reģistrāciju, uzskaiti un saslimstības analīzi,
 - b) cilvēku, dzīvnieku un vides materiālu laboratoriskās pārbaudes infekcijas slimību izraisītāju cirkulācijas novērošanai,
 - c) iedzīvotāju imunitātes izpēti;
3. nodrošināšanu ar imūnbioloģiskiem preparātiem un iedzīvotāju vakcināciju;
 4. slimnieku un infekciozo personu atklāšanu, uzskaiti, ārstēšanu un, ja nepieciešams, izolēšanu;
 5. kontaktpersonu noteikšanu, uzskaiti, laboratoriskās pārbaudes un medicīnisko novērošanu;
 6. īpašu piesardzības un ierobežošanas pasākumu noteikšanu, tajā skaitā profesionālās darbības un piedalīšanās mācību procesā ierobežošanu un aizliegšanu, slimniekiem, infekciozajām personām, kontaktpersonām un personām, par kurām ir radušās epidemioloģiski pamatotas aizdomas, ka tās ir atradušās paaugstināta inficēšanās riska apstākļos;
 7. infekcijas slimību perēkļu atvēršanas pasākumus, kā arī pasākumus infekcijas slimību izraisītāju cirkulācijas pārtraukšanai ārējā vidē;
 8. sabiedrības veselības aizsardzības pasākumus;
 9. iedzīvotāju informēšanu par epidemioloģisko situāciju un izglītošanu infekcijas slimību profilakses jautājumos;
 10. likumā noteikto piespiedu līdzekļu piemērošanu par epidemioloģiskās drošības pasākumu nepildīšanu.

LĀSIS 5. panta 1. daļa nosaka, ka Ārkārtas situāciju Ministru kabinets var izsludināt uz laiku ne ilgāku par trīs mēnešiem.



Ilustrācija 7 Analizējamie periodi un atskaites punkti

Ārkārtas stāvokļa izsludināšana notika pēc Pasaules veselības organizācijas 11.03.2020. paziņojuma, ka Covid-19 ir sasniegusi pandēmijas apmērus ar mērķi ierobežot Covid-19 izplatību ārkārtējās situācijas spēkā esamības laikā.

Ārkārtas situācijas izsludināšanas brīdī no epidemioloģiskās drošības viedokļa pastāvēja katastrofas draudi, kad „risku novērtējums, prognozes, informācija vai citi apstākļi pamatoti liecināja par katastrofas iespējamību”.

Epidēmijas ekonomiskie riski atšķiras no epidemioloģiskajiem riskiem. COVID-19 gadījumā, finansiālā un institucionālā kapacitāte ir būtiskākais priekšnoteikums ekonomikas noturībai šoka apstākļos (Noy, Doan, & Benno, 2020).

Ministru kabineta 12.03.2020. rīkojums nr.103. (turpmāk Rīkojums nr.103) „Par ārkārtējās situācijas izsludināšanu” paredzēja virkni ierobežojumu epidemioloģiskās drošības nodrošināšanai, kas būtiski ietekmēja uzņēmējdarbību:

- ierobežoja pulcēšanos pēc cilvēku skaita gan iekštelpās, gan ārpus tām;
- ierobežoja pulcēšanās pieļaujamo ilgumu, kā arī noteica pulcēšanās aizliegumus nakts stundās;

- noteica sociālās distancēšanās prasības publiskās vietās, kas ietekmēja pieļaujamo apmeklētāju skaitu sabiedriskās ēdināšanas uzņēmumos utt. (Noteikumu nr.104 4.5., 4.5¹., 4.5.²pnkt.)
- noteica prasības ievērot pašizolācijas prasības personām, kas atgriezušās no ārvalstīm u.c.

Šīs prasības radīja ekonomiskas grūtības virknei uzņēmumu, īpaši tiem, kas strādā tūrisma, transporta un sabiedriskās ēdināšanas nozarēs. Piemēram, kopš 2020. gada marta vidus līdz ar robežu slēgšanu, lidojumu un starptautisko pasažieru pārvadājumu pārtraukšanu tūrisma mārketinga aktivitātes praktiski tika izbeigtas un tūristu skaits dramatiski saruka, kā rezultātā jau 1.ceturksnī Latvijas tūrisms piedzīvoja kritumu par 13%. Aprīlī viesu skaita sarukums sasniedza jau 94% (Pelēce, 2020). Publisko pasākumu aizliegumi, pulcēšanās un mobilitātes ierobežojumi tieši un uzreiz apturēja aktivitāti vairākās nozarēs. Izmitināšanas un ēdināšanas nozares un atpūtas un izklaides pakalpojumu nozares pievienotās vērtības kritums 2. ceturksnī lēšams tuvu 70%, bet 2020. gadā kopumā šajās nozarēs kritums varētu sasniegt aptuveni 30-50%, kas ir pozitīvāk salīdzinājumā ar izredzēm, kas tiek prognozētas tūrismam globālā mērogā (58-78%) (Pelēce, 2020).

Pēc ārkārtējās situācijas beigām epidemioloģiskās drošības pasākumus nosaka Ministru kabineta 09.06.2020.noteikumi nr.360 "Epidemioloģiskās drošības pasākumi Covid-19 infekcijas izplatības ierobežošanai", kas saglabā pulcēšanās ierobežojumus, definē prasības distances ievērošanai, nosaka prasības un priekšnosacījumus izolācijai, pašizolācijai un karantīnai.

Tas nozīmē, ka COVID-19 pandēmijas radītie ierobežojumi lielā mērā saglabājas arī pēc ārkārtējās situācijas beigām. Covid-19 infekcijas izplatības pārvaldības likuma pārejas noteikumu 10.punkts nosaka "Šis likums ir spēkā tik ilgi, kamēr pastāv epidemioloģiskās drošības draudi saistībā ar Covid-19 infekcijas izplatību. Ministru kabinets vismaz reizi trijos mēnešos sniedz Saeimai ziņojumu par epidemioloģiskās drošības draudiem saistībā ar Covid-19 infekcijas izplatību. Saeima atzīst šo likumu par spēku zaudējušu ar atsevišķu likumu".

Tātad - visu laiku, kamēr būs spēkā epidemioloģiskās drošības ierobežojumi, pastāvēs uzņēmējdarbības riski, kas saistīti ar šiem ierobežojumiem.

Pandēmijas gaitā Ministru kabinets ar 06.11.2020. rīkojumu nr.655 atkārtoti izsludināja ārkārtējo situāciju un paredzams, ka dažādi ierobežojumi pastāvēs līdz brīdim, kamēr epidemioloģiskā situācija būtiski uzlabosies.

Līdz ar to, laika griezumā (skat.7.ilustrāciju) uzskatāms, ka šobrīd Latvija atrodas pandēmijas/ārkārtējās situācijas periodā, kur būtiska ir atbalsta pasākumu plānošana un operatīva ieviešana krīzes seku mazināšanā uzņēmējdarbībā un ekonomikā kopumā.

2.2. Krīzes pārvaldības principi

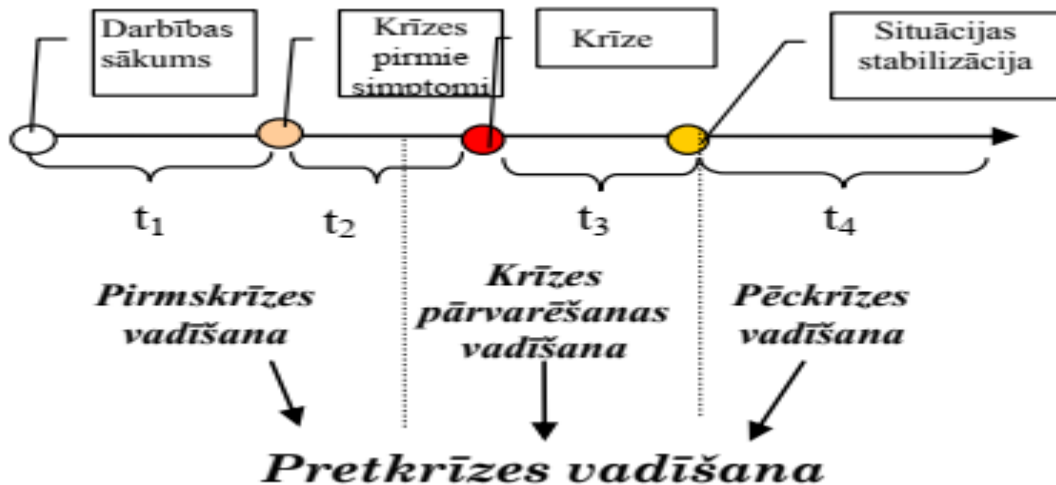
Saimnieciskās darbības samazināšanās, kas aizsākās ar epidemioloģiskās drošības pasākumu ieviešanu, izvērtās ekonomiskajā krīzē, kuras pārvaldībai ir nepieciešamas efektīvas metodes.

Uzņēmuma krīzes dzīves cikls iedalāms šādos posmos (Mogorite & Didenko, 2012):

1. Sākums jeb snaudošā krīzes fāze. Ja šajā gadījumā nav veiktas nepieciešamās darbības krīzes apturēšanai, tad šīs fāzes vēlamais rezultāts ir sagatavošanās nākamajai stadijai;
2. Straujā krīzes fāze, kad situāciju nav iespējams novērst. Notiek uzņēmumu rezervju krasa samazināšanās. Ja rezervju nav, uzreiz notiek pāreja uz nākamo fāzi;

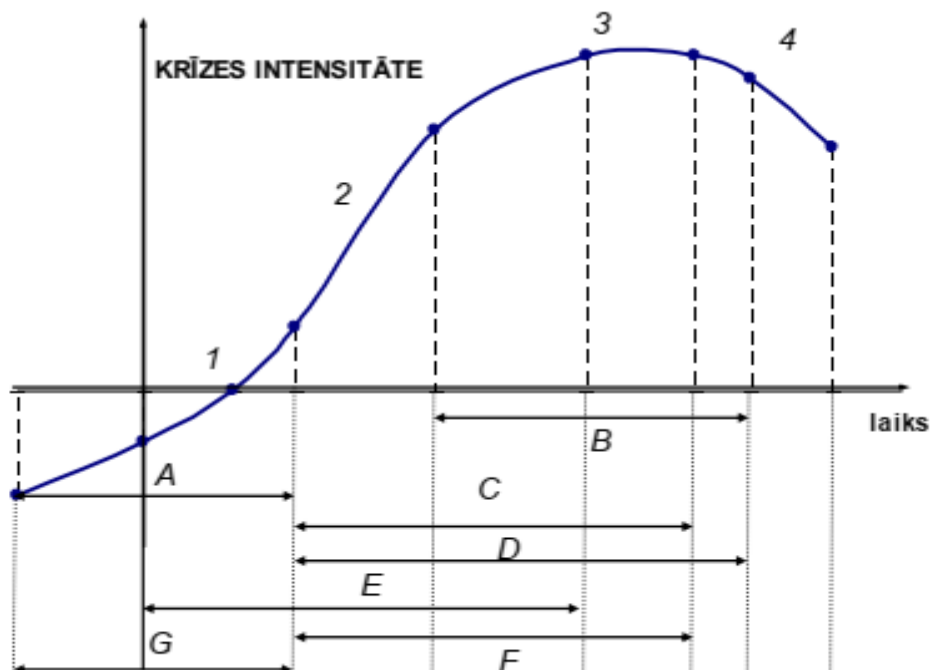
3. Hroniska krīze. Atsevišķi autori to nosauc par krīzes kulmināciju, kam raksturīga maksātnespēja, finansiāla nestabilitāte, hronisks apgrozāmo līdzekļu trūkums. Krīzes pārvaldības uzdevums ir samazināt šo fāzi līdz minimumam;
4. Krīzes atrisinājuma fāze, kurā pozitīva iznākuma gadījumā ir iespējams nonākt kvalitatīvi citā līmenī vai arī iestājas negatīvais iznākums – uzņēmuma likvidācija.

Uzņēmuma pretkrīzes vadīšanai var izdalīt 3 posmus (Mogorite & Didenko, 2012): pirmskrīzes vadīšana, krīzes pārvarēšanas vadīšana un pēckrīzes vadīšana.



Ilustrācija 8 Pretkrīzes vadīšanas struktūra (Mogorite & Didenko, 2012)

- t₁ – informācijas vākšana un novērošana;
- t₂ – novērošana un pirmo pazīmju pārvarēšana;
- t₃ – pārvarēšanas pasākumi, negatīvo ietekmju samazināšana;
- t₄ – situācijas stabilizēšana, kontroles pasākumi.



Ilustrācija 9 Uzņēmuma krīzes dzīves cikls un krīzes pārvarēšanas stratēģijas (Mogorite & Didenko, 2012)

A - krīzes novēršanas stratēģija, pirmskrīzes vadīšana;

B - gaidīšanas stratēģija, krīzes brieduma nogaidīšana pārvarēšanas problēmu veiksmīgai risināšanai;

C - pretdarbība krīzes parādībām, efektīvu lēmumu pieņemšanas stratēģija;

D - situācijas stabilizēšana;

E - risku aprēķināšana un analīze;

F - secīga krīzes pārvarēšana;

G - krīzes seku paredzēšana un nosacījumu radīšana to novēršanai.

Šobrīd nav šaubu par ekonomiskās krīzes esamību. Finanšu ministrija norāda (Latvijas Republikas Finanšu ministrija, 2020): „Latvijas ekonomika pirmo COVID-19 krīzes vilni ir pārvarējusi daudz labāk, nekā tika sagaidīts, un ekonomikas kritums arī 2020. gadā kopumā būs mazāks par jūnijā prognozētajiem 7%, tālākās attīstības perspektīvas pašlaik nav iepriecinošas.”.

Par ekonomikas iespējamu turpmāku lejupslīdi liecina arī Eiropas Komisijas veidotais ESI ekonomiskās pārliecības indekss (ESI). Latvijā ESI indekss ir samazinājies, pasliktinoties gan rūpnieku, gan būvnieku, gan pakalpojumu sektora uzņēmēju noskaņojumam (Latvijas Republikas Finanšu ministrija, 2020).

Nemot vērā, ka šobrīd nav iespējams noteikt, kurā brīdī būs iespējams būtiski samazināt uzņēmējdarbības ierobežojumus, kas noteikti epidemioloģiskās situācijas dēļ, uzmanība jāpievērš tādām krīzes pārvaldības stratēģijām kā risku novērtēšana un analīze (E), kā arī secīga krīzes pārvarēšana (F).

2.3. Risku analīzes pieeja

Risku analīzes ietvars sastāv no šādiem elementiem: bīstamība, iedarbība, ievainojamība un noturība. Uzņēmumu un pakalpojumu noturība šajā ietvarā tiek definēta kā ekonomikas spēja atgriezties iepriekšējā stāvoklī pēc šoka (kurš radies ārējo apstākļu bīstamības, iedarbības un sistēmas ievainojamības rezultātā) (Noy, Doan, & Benno, 2020).

Lemjot par valsts atbalsta pasākumiem uzņēmējdarbībai, ir skaidri un kompleksi jāapzinās mērķis, ko plānots sasniegt šo pasākumu realizācijas rezultātā.

Pieņemot, ka valsts atbalsta mērķis ir uzņēmējdarbības noturība, atbalsta programma jāveido kā risku mazināšanas pasākumu kopums, kas veicina ekonomikas izeju no krīzes un atgriešanos normalitātē.

Lai izveidotu šādu atbalsta programmu, kas balstīta risku novērtējumā, jāveic uzņēmuma risku novērtējums un jāizvērtē kontekstuālie jeb vides riski.

Uzņēmējdarbības risku novērtēšana **uzņēmuma līmenī** ir jāveic, izpildot četrus secīgus posmus:

1. Risku identificēšana un novērtēšana. Risku novērtēšanas process identificē: draudus un to ietekmi uz sabiedrību, risku iestāšanās varbūtību un seku smagumu. Šī procesa

rezultātā katrs drauds tiek identificēts, aprakstīts, analizēts un klasificēts pēc tā iestāšanās iespējamības (P.Coppola, 2015).

Šim posmam vajadzētu sniegt atbildes vismaz uz šādiem jautājumiem (Mullen et al., 2020):

- a. Vai konkrētais darbības veids (business) prasa liela cilvēku skaita uzturēšanos vienā telpā vienlaicīgi?
- b. Vai biznesa vajadzībām nepieciešami daudzi iekšzemes komandējumi?
- c. Vai biznesa vajadzībām nepieciešami starptautiski komandējumi?
- d. Vai biznesam ir nepieciešama tieša saskare ar klientiem vai plašām sabiedrības masām kopumā?
- e. Vai biznesam nepieciešama izejvielu, materiālu vai preču apstrāde un nodošana starp darbiniekiem, klientiem vai citiem sabiedrības locekļiem?
- f. Vai biznesam procesu izpildei nepieciešamas virsmas, kurām pieskaras daudz cilvēku;
- g. Vai biznesam nepieciešams ilgstošs kontakts starp darbiniekiem, piegādātājiem, klientiem vai citiem sabiedrības locekļiem (t.i., vairāk nekā 10 minūtes, mazāk nekā 2 metri);
- h. Vai darbinieki personīgi strādā ar konkrētiem, nedaudziem klientiem, piegādātājiem vai citiem sabiedrības locekļiem katru dienu;
- i. Vai darbinieki personīgi mijiedarbojas ar daudziem klientiem, piegādātājiem, sabiedrības locekļiem katru dienu;
- j. Vai business ikdienā strādā ar īpaši ievainojamām iedzīvotāju grupām (vecu ļaužu aprūpe, cilvēki ar kustību traucējumiem utml.)?

Atbildes uz šiem jautājumiem jāpārvērš kvantificējamās lielumos, piešķirot tām noteiktu svaru punktu izteiksmē.

2. Pielāgojumu (modifikāciju) novērtējums. Šai fāzei būtu jāsniedz atbildes uz šādiem jautājumiem (Mullen et al., 2020):

- a. Vai iespējama biznesa „pārvešana” tiešsaistes režīmā pilnībā?
- b. Vai ir iespējams nozīmīgi samazināt cilvēku skaitu (darbinieki, klienti, piegādātāji, sabiedrība kopumā), kuri ik dienas kontaktējas personīgi. Tas var iekļaut tādus pasākumus kā:
 - i. Produkcijas pasūtīšana tiešsaistē un piegāde bez tieša kontakta (*pick up*);
 - ii. Ārtelpu izmantošana, lai samazinātu kontaktus iekštelpās;
 - iii. Cilvēku skaita ierobežošana, kuri iekštelpās uzturas vienlaicīgi;
 - iv. Vienlaikus apkalpojamo klientu skaita ierobežošana;
 - v. Tiešo kontaktu (*face to face*) ierobežošana starp darbiniekiem, piegādātājiem un klientiem;
 - vi. Alternatīva darba laika piedāvāšana klientiem, lai ierobežotu vienlaicīgi apkalpojamo klientu skaitu.
- c. Vai iespējams būtiski samazināt iekšzemes un starptautisko komandējumu skaitu?
- d. Vai iespējams ieviest fiziskās distancēšanās pasākumus, piemēram
 - i. Atzīmes uz grīdas distancē ievērošanai;
 - ii. Fiziskas barjeras vai vairogi starp darbiniekiem vai starp darbiniekiem un klientiem.
- e. Vai business var tikt modificēts tā, lai ierobežotu lielas sanāksmes, konferences, sacensības utml. pasākumus;

- f. Vai bizness var tikt modificēts tā, lai būtiski ierobežotu saskari starp darbiniekiem, klientiem un piegādātājiem, t.sk.
 - i. Pārejot tikai uz tiešsaistes pakalpojumiem;
 - ii. Izveidojot politikas noteiktām preču grupām, kad pieļaujams, ka neatbilstoša prece netiek atdota (nosūtīta) atpakaļ (non return policy);
 - iii. Piedāvājot maksājumus veikt tikai tiešsaistē;
 - iv. Nodrošinot darbiniekus ar personīgās aizsardzības līdzekļiem.
3. Kopējais novērtējums, punktu izteiksmē ievērojot riskus un modificējošos pasākumus;
4. Balstoties uz iepriekšējo novērtējumu ir jāpieņem lēmumi par risku mazināšanas pasākumiem (Mullen et al., 2020):
 - a. Fizisko distancēšanos starp personām (Person-to-Person);
 - b. Fizisko distancēšanos starp personām un objektiem, kurus lieto (kam pieskaras) citas personas (Person-to-Shared objects);
 - c. Sanitārijas un Higiēnas pasākumi;
 - d. Uzņēmumu politikas pasākumi;
 - e. Riska komunikācijas pasākumi.

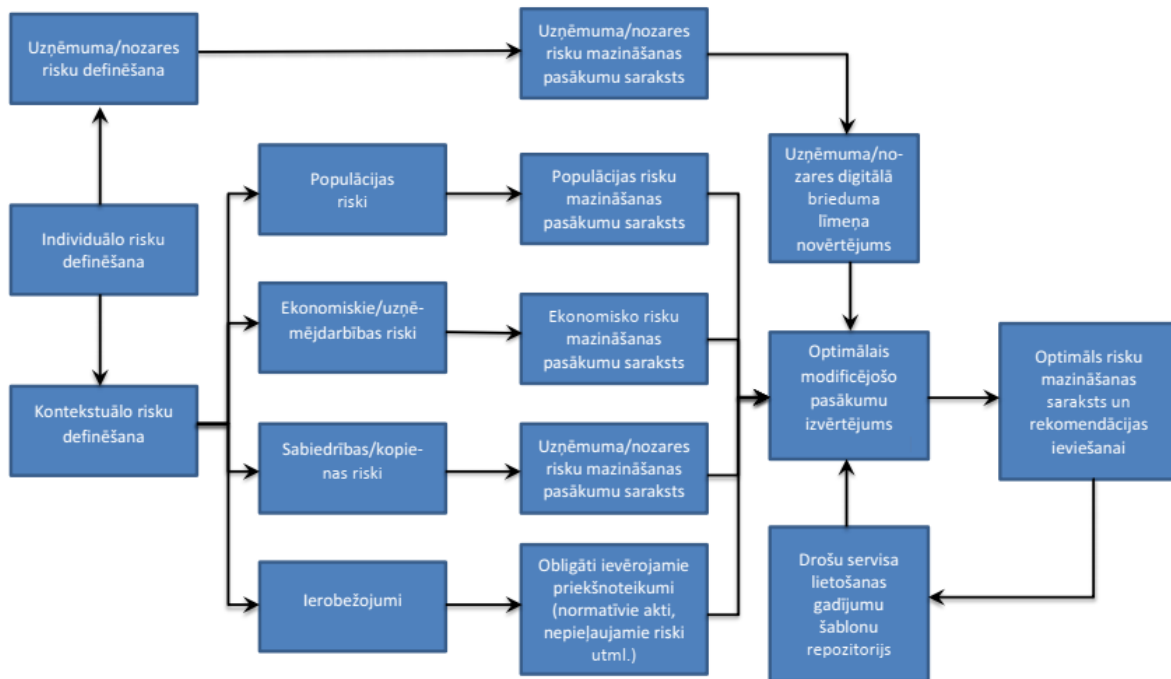
Risku mazināšanas pasākumu identificēšanai ir izmantojama zināšanu bāze (saite uz zināšanu bāzi), kas izveidota zināšanu apmaiņai šablonu veidā ātrai zināšanu uzkrāšanai par krīzes seku pārvarēšanas risinājumiem (šablonu piemēri iekļauti 3.pielikumā).

Katra individuālā uzņēmuma risku izvērtējums ir tikai viens no faktoriem, kas jāņem vērā, lemjot par atbalsta pasākumiem COVID 19 izraisītās krīzes seku mazināšanā. Paralēli uzņēmuma riskiem, katrs uzņēmumā strādājošais saskaras ar individuālajiem riskiem, grūtības uzturēt darbu un privātās dzīves līdzsvaru un mentālās veselības problēmas sociālās izolācijas un ekonomiskās nedrošības dēļ (Kantar, 2020). Arī šie riska faktori ir jāņem vērā un jāvērtē kopā ar uzņēmuma riskiem, gan arī raugoties visas sabiedrības kontekstā.

Institūcijām, kas atbild par krīzes pārvaldību un pieņem lēmumus par pasākumiem krīzes seku mazināšanā ir jāizstrādā risku novērtēšanas kritēriji, ņemot vērā ne tikai konkrētā uzņēmuma riskus un to mazināšanas pasākumus, bet arī kontekstu. Izstrādājot kontekstuālos risku analīzes kritērijus, jāņem vērā politiskā, sociālā, juridiskā un fiziskā vide, kurā var realizēties apdraudējums. Šie kritēriji ietver (P.Coppola, 2015):

1. Populācijas apsvērumus:
 - a. Miršanu un ievainojumus;
 - b. Iedzīvotāju pārvietošanos;
 - c. Māju un īpašuma zaudēšanu;
 - d. Darba un ienākumu zaudēšanu;
 - e. Drošības sajūtas zudumu;
 - f. Kopības izjūtas zudumu.
2. Uzņēmējdarbības apsvērumus:
 - a. Objektu bojājumus;
 - b. Ienākumu zaudēšanu;
 - c. Biznesa sagraušanas izmaksas;
 - d. Tirgus daļu zaudēšanu;
 - e. Apmācītu darbinieku zaudēšanu;
 - f. Bankrotus.
3. Sabiedrības (kopienas) apsvērumus:
 - a. Infrastruktūras bojājumus/nepieejamību (ceļi, tilti, slimnīcas, cietumi, iestādes, klientu apkalpošanas centri utt.);
 - b. Nodokļu ieņēmumu zaudēšanu;
 - c. Reakciju uz krīzi un atkopšanās izmaksas;

- d. Finansējuma samazināšanos citām sabiedrības prioritātēm, piemēram, izglītībai, sociālajai palīdzībai utml.;
- e. Iedzīvotāju bāzes zudumu;
- f. Pieaugošu kopienas parādu un aizņēšanās;
- g. Ekonomisko atsitienu;
- h. Kaitējumu apkārtējai videi;
- i. Kultūras/ vēsturiskā mantojuma zaudēšanu.



Ilustrācija 10 Risku analīzes metodiskais ietvars uzņēmumu darbības noturībai

3. Esošā situācija rīcībpolitikas jomā

Laiks no 2020. gada 12. marta, kad tika izsludināta ārkārtas situācija līdz 2020. gada 10. jūnijam, kad stājās spēkā likums “Epidemioloģiskās drošības pasākumi Covid-19 infekcijas izplatības ierobežošanai” ir uzskatāms iezīmē pārejas posmu, kas iezīmē būtiskas izmaiņas sabiedrībā kopumā, t.sk. sabiedrības attieksmē un rīcībpolitikā, kas attiecas uz attālināto darbu un digitālo transformāciju.

3.1. Attālinātais darbs

3.1.1. Normālā situācijā

Dažādu valstu, nozaru un profesiju pieredzes attālinātā darba izmantošanā/nodrošināšanā pirms krīzes var sniegt informāciju par tā plašākām izmantošanas iespējām, kā arī par faktoriem, kas ļauj novērst neefektīvu tā izmantošanu.

Pēdējā desmitgadē ir izstrādātas dažādas attālinātā darba politikas, kuras izstrādātas gan valstu līmenī, gan uzņēmumu līmenī, gan veidoti nacionāli un sociāli dialogi, tomēr starptautiskā līmenī attālinātā darba tēma nav plaši apskatīta, izņemot 2002. gada Eiropas

sociālo partneru Pamatnolīgumā par attālināto darbu (teledarbu) Eiropas Savienībā (turpmāk tekstā – pamatnolīgums) (Eurofound and the International Labour Office, 2017).

Eiropas Savienības līmenī nav izstrādā direktīva, kas konkrēti veltīta attālinātajam darbam, taču šī tēma ir iekļauta gan Eiropas Parlamenta un Padomes direktīvā 2003/88/EK par konkrētiem darba laika organizēšanas aspektiem, gan iepriekš minētajā Pamatnolīgumā. Pamatnolīgumā noteikts, ka darba devējs ir atbildīgs par darbinieka darba aizsardzību saskaņā ar Direktīvu 89/391 un citām saistošajām meitas direktīvām, nacionālo likumdošanu un koplīgumiem (COMMISSION OF THE EUROPEAN COMMUNITIES, 2008). Latvijas sociālie partneri (Latvijas Darba devēju konfederācija, Latvijas Brīvo arodbiedrību savienība) noslēdza vienošanos par Pamatnolīguma ieviešanu 2006. gadā.

Latvijā attālinātais darbs līdz šim nav bijis plaši izplatīts – kopš 2012. gada, kad attālināti bija iespēja strādāt 2%, tas 2019. gadā ir palielinājies līdz 3% no kopējā nodarbināto skaita (Eurostat, 2020). 2020. gada Eurostat pētījums, kas publicēts ar nosaukumu “*How usual is it to work from home?*” jeb “Cik tas ir ierasti strādāt no mājām?” norāda, ka Latvijā to nodarbināto personu īpatsvars, kuras parasti strādā no mājām (3%) ir gandrīz divreiz zemāks nekā vidēji Eiropas Savienībā (5,5%). Tomēr pēdējo 5 gadu laikā ir novērojams to personu, kas izvēlas strādāt attālināti, skaita pieaugums gan Latvijā, gan citās Eiropas Savienības valstīs. Saistībā ar Covid-19 izraisītām sekām Latvijā, visticamāk, to nodarbināto personu īpatsvars, kuras parasti strādā no mājām, palielināsies 2020. gadā (Eurostat, 2020).

Pētījumu un konsultāciju uzņēmuma “Kantar” pētījumā, kas veikts 2015. gadā Latvijā, aptaujājot 800 strādājošos, tika noskaidrots, ka ārkārtējās situācijas laikā strādājošie salīdzinoši visbiežāk (15%) norāda, ka viņiem pietrūkst tiešās saskarsmes ar kolēģiem, klientiem un citiem cilvēkiem. It īpaši tas raksturīgs strādājošajiem, kas ārkārtējās situācijas laikā pilnībā vai daļēji pārgājuši uz darbu attālinātā režīmā. Savukārt 8% atzinīgi izsakās par elastīgo darba laiku un brīvākām laika plānošanas iespējām. Līdzīgi – nedaudz mazāk kā ~1/10 strādājošo novērtē attālinātā darba iespējas kopumā (7%), kā arī to, ka, strādājot attālināti, tiek taupīta nauda un laiks, kas tiek pavadīts ceļā uz un no darba (Kantar, 2020).

Pieaugot digitālās infrastruktūras pieejamībai, pirmie priekšlikumi veicināt attālināto darbu Latvijā tika iekļauti jau 2001. gadā apstiprinātajā Latvijas ilgtermiņa ekonomiskajā stratēģijā. Tāpat priekšlikumi par attālināto darbu tika iekļauti arī 2010. gadā apstiprinātajā Latvijas Ilgtspējīgas attīstības stratēģijā līdz 2030. gadam. Attālinātais darbs Latvijas Ilgtspējīgas attīstības stratēģijā līdz 2030. gadam minēts kā mūsdienīga un elastīga darba forma, kas palīdzētu mazināt depopulāciju. Arī Nacionālais attīstības plāns 2014.-2020. gadam un Reģionālās politikas pamatnostādnes 2013.-2019. gadam uzsver nepieciešamību veicināt attālinātā darba izmantošanu Latvijā (Rīgas Tehniskā universitāte, 2014). Attālinātā darba veicināšana sekmētu saglabāt lauku apdzīvotību, veicinātu informācijas sabiedrības attīstību, samazinātu uzņēmumu infrastruktūras uzturēšanas izmaksas, utt. Neraugoties uz to, ka attālinātais darbs un tā nodrošināšana tika iekļauta nozīmīgos plānošanas dokumentus, tomēr tā izmantošana nav strauji palielinājusies.

Attālinātā darba formu regulē, iekļaujot darba līgumā nosacījumu, ka darbs var tikt veikts attālināti, balstoties Darba likuma 40. pantā ietvertajiem nosacījumiem, ja nav veikti šādi grozījumi, tad jāņem vērā darba likuma 53. panta pirmā daļa, kas norāda, ka darbiniekam ir pienākums veikt darbu uzņēmumā, ja darbinieks un darba devējs nav vienojušies citādi.

Darbiniekam, kurš veic attālināto darbu, jāsadarbojas ar darba devēju darba vides riska novērtēšanā un jāsniedz darba devējam informācija par savas darbavietas apstākļiem, kas var ietekmēt viņa drošību un veselību. Būtiski attālinātā darba īstenošanā, ka darbinieks ievēro darba aizsardzības, elektrodrošības, drošības tehnikas, darba higiēnas un ugunsdrošības, ēku

lietošanas un citus noteikumus. Veicot darbu attālināti, darbinieks uzņemas atbildību, ka viņa darbavieta un aprīkojums ir piemērots darba veikšanai (JANSONS & STIVRIŅA, 2020).

3.1.2. Ārkārtējās situācijas laikā

Neskatoties uz nepārtraukto tehnoloģiju attīstību un globalizāciju, attālinātā darba izmantošana neizplatījās strauji un netika plaši izmantota, taču situācijā mainījās šā gada pavasarī. Sākoties Covid-19 pandēmijai, Eiropas valstis sāka ieviest dažādus sociālās un fiziskās distancēšanās pasākumus, līdz ar to “piespiežot” darba devējam piedāvāt darbiniekam strādāt attālināti (Fana et al, 2020). *Eurofound* norāda, ka 2020. gada aprīlī gandrīz 40% darbinieku ES sāka strādāt pilnībā (pilnu slodzi) attālināti (*Eurofound*, 2020).

Covid-19 pandēmijas rezultātā daudzas Eiropas valsts ieviesa noteikumus vai ieteikumus, lai tiktu ievērota sociālā un fiziskā distancēšanās, piemēram, lūdza izmantot attālināto darbu, noteica stingrākus veselības un drošības pasākumus darba vietā. *Eurofound* izstrādāja *COVID-19 EU PolicyWatch* datu bāzi, kuras mērķis ir kartēt pasākumus, kas ieviesti, lai mazinātu sociālo un ekonomisko ietekmi uz uzņēmumiem, darbiniekiem un iedzīvotājiem. Papildus tajā iekļauta arī informācija par sociālo partneru lomu Covid-19 ietekmes mazināšanas pasākumu izstrādē un īstenošanā. 2020. gada novembrī reģistrēti 805 politikas instrumenti, kas ir ieviesti, lai tiktu atbalstīti iedzīvotāji. Saistībā tieši ar attālināto darbu ir novērotas 20 rīcībpolitiku izmaiņas, piemēram, Austrijā, Luksemburgā, Portugālē, Lietuvā utt. Datu bāzē apkopota informācija par visām Eiropas Savienības valstīm un Norvēģiju, Lielbritāniju (*Eurofound*, <https://www.eurofound.europa.eu>, 2020).

Laiks no 2020. gada 12. marta, kad tika izsludināta ārkārtējā situācija līdz 2020. gada 10. jūnijam, kad stājās spēkā likums “Epidemioloģiskās drošības pasākumi Covid-19 infekcijas izplatības ierobežošanai”, un satraukums, nezināšana sabiedrībā radīja tādas apstākļus, kad darba ņēmēji un darba devēji izvēlējās attālinātā darba sniegtās iespējas.

Latvija Digitālās ekonomikas un sabiedrības indeksā (DESI) ieņem vietu zem Eiropas vidējā rādītāja un it īpaši jāņem vērā norādītais, ka Latvijas uzņēmējdarbības nozarē netiek izmantotas digitālo tehnoloģiju sniegtās iespējas, kā arī vairāk nekā pusei iedzīvotāju nav digitālo pamatprasmju (Eiropas Komisija, Digitālās ekonomikas un sabiedrības indekss (DESI) 2020. gadā Latvija., 2020), līdz ar to šie minētie apstākļi varētu radīt sarežģījumus abām iesaistītajām pusēm – gan darbiniekam, gan darba devējam, nodrošinot attālināto darbu.

5% aptaujāto Latvijas iedzīvotāju norāda, ka viņiem nepatīk attālinātais darbs, jo ir nepietiekošs tehniskais nodrošinājums, laukietilpīgāka un sarežģītāka darba organizācija (Kantar, 2020). Līdzīgi respondenti norādīja arī grāmatvedības un uzņēmuma vadības sistēmas “Tildes Jumis” veiktajā aptaujā par attālināto darbu, kuras ietvaros tika konstatēts, ka attālināti strādāja aptuveni 25% darbinieku, kuru darbā nav nepieciešams fiziski atrasties birojā. Kā galveno iemeslu darba klātienes apmeklēšanai respondenti minēja uzņēmuma vājo digitalizāciju, kur dokumentācija lielākoties ir papīra formātā (Tilde, 2020). Līdz ar to apstiprinās, ka DESI indeksa rezultāti, kas rāda, ka uzņēmumi nespēj vēl efektīvi izmantot digitālās tehnoloģijas un tās integrēt savās sistēmās, lai nodrošinātu labāku attālināto darbu.

Savukārt Latvijas Televīzijas pasūtītajā SKDS aptaujā par attālināto darbu no 30.04.2020. līdz 05.05.2020., tika arī secināts, ka katrs piektais darbinieks Latvijā strādāja attālināti un starp ieguvumiem, ko sniedz attālinātais darbs, tika norādīta iespēja efektīvāk veikt darba uzdevumus, laika ietaupīt, kas tiktu pavadīts dodoties uz dažādām sanāksmes vietām, jo viss ir pieejams datorā (Latvijas Televīzija, 2020).

Uzņēmuma “Tele2” sadarbībā ar “Norstat” 2020. gada ārkārtējās situācijas izsludināšanas laikā veiktajā pētījumā tika identificēts, ka vislielākie attālinātās strādāšanas

piekritēji ir tie, kuri šajā krīzes laikā jau strādāja attālināti (62%), cilvēki vecumā no 18 līdz 39 gadiem, ar vidēji augstiem un augstiem ienākumiem, ar augstāko izglītību, vadītāji (40%), kvalificēti speciālisti (38%) un pašnodarbinātās personas (51%). Pētījumā noskaidrots, ka pēc krīzes beigām strādāt attālināti vairāk vēlas Rīgā (39%) un Pierīgā (36%) dzīvojošie. Vidzemē vēlmi strādāt attālināti pauž 30% iedzīvotāju, Latgalē - 27%, Zemgalē - 25%, bet vismazāk Kurzemē - 24% (Tele2, 2020). Līdz ar to novērojams, ka iedzīvotāji, kuri saskaras ar ilgāku pavadīto laiku ceļā uz un no darba, izvēlētos strādāt attālināti.

Jāņem vērā, ka pirmās ārkārtas situācijas laikā, kas Latvijā sākās 2020. gada 16. martā un beidzās 2020. gada 10. jūnijā neviens ārējais normatīvais akts konkrēti neregulēja attālināto darbu. Iespēja noteikt attālināto darbu darba devējiem pastāvēja, to iekļaujot darba kārtības noteikumos, kuros varēja atrunāt kāda veidā tiek organizēts darba laika laiks, sasniedzamības iespējas, darba aizsardzības prasību ievērošana. Neraugoties uz to, ka nebija vēl izstrādāts neviens normatīvais akts darba devējiem pastāvēja iespēja nodrošināt darbiniekam attālināto darbu, veicot darba līguma grozījumus, kas jau tika minēti iepriekšējā apakšnodaļā.

3.1.3. Atkopšanās situācijā

Covid-19 radītā krīze lielā mērā ir paātrinājusi uzņēmējdarbības digitalizāciju. Daudzi ir spējuši ātri reaģēt un pārorientēt savu biznesu uz mainīgajiem apstākļiem, digitalizēt piegādes pakalpojumus un daudz ko citu, radot un piedāvājot jaunus, novatoriskus produktus un risinājumus tādās jomās kā veselības aprūpe, e-komercija un loģistika. Šobrīd krīzes situācijas iespaidā ieradumu maiņa sabiedrībā notiek strauji.

Grozījumi Darba aizsardzības likumā, kuros definēts attālinātais darbs, tika izstrādāti un valdība tos atbalstīja jau 2018. gada novembrī, taču Saeima tos pieņēma 2019. gada oktobrī, nosakot spēkā stāšanās laiku – 2020. gada 1. jūliju. Likumā tika iekļauts darba aizsardzības regulējums attālinātajam darbam, jo, kā pamatojusi grozījumu izstrādātāja Labklājības ministrija: aizvien aktuālākas kļūst dažādas specifiskas nodarbinātības formas, arī attālinātais darbs, tādēļ ir nepieciešams darba aizsardzības prasības konkretizēt, lai nodrošinātu pēc iespējas drošu darba vidi visiem nodarbinātajiem (Dārziņa, 2020). Jāņem vērā, ka šo likuma grozījumu stāšanās spēkā sakrita ar strauji pieaugošu nepieciešamību regulēt attālināto darbu, jo krīzes rezultātā palielinājās to personu un darba devēju skaits, kas izvēlējās attālināto darbu. Papildu attālinātā darba definīcijai, darba aizsardzības likumā pēc 1. jūlijā tika precizēta arī ar darba aizsardzību saistīto procesu dokumentēšana un dokumentu parakstīšana ar elektronisko parakstu, pašnodarbinātā darba drošības prasības un to ievērošana, darba aizsardzības struktūras lielajos, bīstamo nozaru uzņēmumos. Visi minētie grozījumi uzlabo darbinieku apstākļus attālinātā darbā.

Darba aizsardzības likumā, kura grozījumi stājās spēkā 2020. gada 1. jūlijā, tika definēts attālinātais darbs, kur norādīts, ka tas ir tāds darba izpildes veids, kurā darbs, ko nodarbinātais varētu veikt darba devēja uzņēmumā, pastāvīgi vai regulāri tiek veikts ārpus uzņēmuma, tas ir arī darbs, ko veic, izmantojot informācijas un komunikācijas tehnoloģijas. Par attālināto darbu šā likuma izpratnē netiek uzskatīts darbs, kas ir saistīts ar regulāru pārvietošanos.

Darba aizsardzības likuma grozījumu anotācija paskaidrots, ka attālinātais darbs šā likuma izpratnē attiecas ne tikai uz darbu ar datoru, bet arī jebkuru citu darbu ārpus uzņēmuma, piemēram, tā var būt kādu lietu izgatavošana vai apstrāde darba devēja uzdevumā. Vienlaikus tiek uzsvērta robežšķirtne: par attālināto darbu tiek uzskatīts tikai tas darbs, kuru var veikt uzņēmuma darba vietās, bet pēc darba devēja un nodarbinātā savstarpējas

vienošanās darbinieks to pastāvīgi vai regulāri veic mājās vai citā darba vietā. Turklāt darbs var tikt veikts arī vairākās darba vietās, pārvietojoties, privātās vai publiskās vietās, kopstrādes telpās vai reizēm arī ārpus telpām. Par attālināto netiek uzskatīts darbs, kas saistīts ar regulāriem un sistemātiskiem izbraukumiem un pārvietošanos, piemēram, piegādes un pārvaldījumu pakalpojumi, izbraukumi pie klientiem, komandējumi un darba braucieni (Latvijas Republikas Ministru kabinets, 2020).

Savukārt 2020. gada 5. jūnijā pieņemtie likumi Covid-19 infekcijas izplatības seku pārvarēšanas likums un Covid-19 infekcijas izplatības pārvaldības likums stājās spēkā 10. jūnijā, kad tika pārtraukta ārkārtas situācija, un ir vēl aizvien spēkā esoši. To mērķis ir atjaunot vispārējo tiesisko kārtību pēc noteiktā ārkārtējās situācijas termiņa beigām, paredzot atbilstošu pasākumu kopumu Covid-19 infekcijas izplatības seku pārvarēšanai un īpašos atbalsta mehānismus un izdevumus, kas tieši saistīti ar Covid-19 izplatības ierobežošanu, lai nodrošinātu sabiedrības ekonomiskās situācijas uzlabošanu un veicinātu valsts tautsaimniecības stabilitāti. Papildu atbalsta mehānismu ieviešanai, infekcijas pārvaldības likuma mērķis ir nodrošināt efektīvu valsts institūciju darbību saistībā ar Covid-19 izplatību.

MK noteikumi Nr.360 "Epidemioloģiskās drošības pasākumi Covid-19 infekcijas izplatības ierobežošanai" (pieņemti 09.06.2020, stājās spēkā 10.06.2020) nosaka, ka atbilstoši iespējām un darba specifikai, distancēšanās prasību nodrošināšanai ir jāveicina darba veikšana attālināti. Tas attiecināms arī uz attālinātu saimniecisko vai publisko pakalpojumu sniegšanu un izmantošanu (pieteikšanās pakalpojumam attālināti, biļešu tirdzniecība internetā).

Šobrīd atkopšanās posmā tiek gatavoti Ministru kabineta noteikumi saistībā ar attālinātā darba izmaksu kompensēšanu, kas paredzēs mēneša normu, kuru nepārsniedzot izdevumi netiek papildus aplikti ar nodokli (Pumpiņš, 2020).

Nemot vērā, visu iepriekš minēto var secināt, ka ārkārtējās situācijas laikā gūtās atziņas tiek ņemtas vērā un tiek meklēti atbilstoši risinājumi, lai uzlabotu un papildinātu rīcībpolitiku.

3.1.4. Jaunajā normālajā situācijā

Digitālais risinājums attālinātā darba veikšanai nav jāuztver kā vienreizējs, specifisks problēmu risināšanas rīks, bet gan kā sistemātiska pieeja, lai veicinātu produktivitāti un ilgtermiņa konkurētspēju.

OECD norāda, ka pēc Covid-19 pandēmijas izraisītajiem izaicinājumiem darba vidē, ir nepieciešams izstrādāt tādas politikas, kas maksimizēs ekonomiskos labumus un veicinās produktivitāti attālinātajā darbā. **Pirmkārt, jāizstrādā tāda politika, ka attālinātais darbs var būt izvēle. Otrkārt, jāizstrādā tāda politika, kas nodrošinās darbiniekam piemērotu darba vidi attālinātā darba veikšanai. Treškārt, jāizstrādā politika, kas attīsta labākās vadīšanas prakses attālinātā darba nodrošināšanai. Un ceturtkārt, jauno politiku izstrādē nepieciešams pievērst uzmanību ātras, uzticamas un drošas IKT infrastruktūras izveidošana un attīstīšanai** (OECD, Productivity gains from teleworking in the post COVID-19 era : How can public policies make it happen?, 2020).

Līdzīgi kā OECD arī neseno veiktajā Eiropas Komisijas Kopīgā pētniecības centra pētījumā par attālināto darbu tā organizēšanu un darba kvalitāti Covid-19 krīzē, tika secināts, ka jaunajā normālajā situācijā nepieciešams uzlabot iespējas izvēlēties, kad strādāt attālināti un kad klātienē, uzlabot darba devēju darba stilu (pastāv nevēlēšanas zaudēt kontroli), uzlabot darba apstākļus, strādājot attālināti (Fana et al, 2020).

Ārkārtas situācijas radītie apstākļi, ierobežojumi un kopējā globālā situācija pasaulē par un ap vīrusu ir radījusi izmaiņas sabiedrības attieksmē un emocionālajā noskaņojumā (Kantar, Koronavīrusa radītā situācija joprojām ietekmē 31% Latvijas iedzīvotāju ikdienu un turpina ietekmēt sabiedrības uzvedību, 2020):

- “Cilvēki pēc atšķirtības lielāku nozīmi piešķir attiecībām ar tuviniekiem un turpmāk lielāku uzmanību plāno veltīt tuviem cilvēkiem un savstarpējām komunikācijām;
- Tāpat pēc izolācijas lielāka nozīme tiek piešķirta dzīves un noteiktu mirkļu baudīšanai;
- Attālinātais darbs liek padomāt par darba un personīgās dzīves līdzsvarošanu;
- Plāno vairāk izvērtēt savus pirkumus un iepirkties ne tik spontāni.”

“Kantar” aptaujā 33% respondentu norādīja, ka pēc Covid-19 pandēmijas centīsies līdzsvarot darbu un personīgo dzīvi (Kantar, Koronavīrusa radītā situācija joprojām ietekmē 31% Latvijas iedzīvotāju ikdienu un turpina ietekmēt sabiedrības uzvedību, 2020), kas norāda, ka attālinātais darbs paliks arvien aktuālākās un rīki tā nodrošināšanai būs nepārtraukti jāmodernizē.

Jāmin, ka arī nākamā plānošanas perioda vadmotīvs “Paradumu maiņa - ceļš uz attīstību!”, kas izklāstīts Nacionālajā attīstības plānā 2021.-2027. gadam. Tas uzsver attālinātā darba nozīmi nākotnē. Attālinātā darba nozīmīgums ir ietverts prioritātes “Stipras ģimenes, veseli un aktīvi cilvēki” nodrošināšanas uzdevumā – “Labvēlīgu apstākļu radīšana ģimenes un darba dzīves saskaņošanai, atbalstot elastīgā un attālinātā darba iespējas, veidojot ģimenei un darba ņēmējam draudzīgu darba vidi un pilnveidojot atbalstu ģimenes aprūpes pienākumu veikšanā.” (Pārresoru koordinācijas centrs, Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam., 2020). Nacionālajā attīstības plānā arī tiek norādīts, ka netiek pilnvērtīgi izmantoti dažādi nodarbinātības veidi, tajā skaitā digitalizācijas ietekmē radītie – attālinātais darbs, platformu ekonomika, automatizācija, nepilna laika nodarbinātība u. c. Tiek norādīts, ka turpmāk nepieciešams veikt pasākumus jauno nodarbinātības veidu pareizai, taisnīgai un efektīvai izmantošanai, lai tiktu izveidoti tādi noteikumi, kas būtu skaidri un godīgi pret abām pusēm – darbinieku un darba devēju (Pārresoru koordinācijas centrs, Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam., 2020).

3.2. Digitālā transformācija

3.2.1. Normālajā situācijā

IKT izmantošana publiskās pārvaldes modernizācijā un publisko pakalpojumu sniegšanā ilgstoši ir bijusi viena no prioritātēm Latvijas publiskajā pārvaldē.

01.01.2003. Saeima apstiprināja elektronisko dokumentu likumu, tādējādi liekot pirmos pamatus juridiski pilnvērtīgu dokumentu izstrādei elektroniskā formā. Elektroniskā paraksta tehnoloģiju attīstība un ieviešana dzīvē aizņēma ilgu laiku, taču soli pa solim tā izmantošana tika uzsākta gan publisko, gan privāto tiesību jomā.

2013. gadā tika apstiprināta koncepcija par publisko pakalpojumu sistēmas pilnveidi, kuras viens no uzdevumiem bija ieviest „vienas pieturas” aģentūras principu valsts un pašvaldību pakalpojumu sniegšanā, tai skaitā, izmantojot informācijas tehnoloģiju iespējas un panākot, ka konkrēta pakalpojuma saņemšanai iedzīvotājiem un uzņēmējiem nebūs jāvērsas vairākās institūcijās un/vai pakalpojumu centros (VARAM, Koncepcija par publisko pakalpojumu sistēmas pilnveidi, 2013).

Īstenojot šajā koncepcijā definētos uzdevumus, tika sagatavoti un iesniegti Saeimā grozījumi Valsts pārvaldes iekārtas likumā, kas deleģēja Ministru kabinetam tiesības noteikt vienotu kārtību publisko pakalpojumu pārvaldības un elektronizācijas jomās, kā arī koordinēt vienoto valsts un pašvaldību klientu apkalpošanas centru darbu (likuma 97-100. panti).

Balstoties uz šo deleģējumu, Ministru kabinets 17.07.2017. apstiprināja šādus noteikumus:

- Nr. 399 Valsts pārvaldes pakalpojumu uzskaites, kvalitātes kontroles un sniegšanas kārtība;
- Nr. 400 Valsts pārvaldes pakalpojumu portāla noteikumi;
- Nr. 401 par valsts pārvaldes vienoto klientu apkalpošanas centru veidiem, sniegto pakalpojumu apjomu un pakalpojumu sniegšanas kārtību;
- Nr. 402 Valsts pārvaldes e-pakalpojumu noteikumi.

Šie noteikumi tiesiski nostiprināja un veicināja publiskās pārvaldes pakalpojumu sniegšanu elektroniskā formā, tajā pašā laikā saglabājot iedzīvotājiem iespēju pieprasīt un saņemt šos pakalpojumus arī izmantojot ierastos klientu apkalpošanas kanālus klātienē un pa pastu.

Nacionālās attīstības plāns (NAP) 2014.-2020. kā vienu no rīcības virzieniem paredzēja nodrošināt pakalpojumu ērtu pieejamību elektroniskā veidā (Pārresoru koordinācijas centrs, Nacionālās attīstības plāns 2014.-2020, 2013), t.sk. plānojot uzdevumus digitālā satura un citu produktu veidošanai, e-pakalpojumu attīstībai, tādejādi paplašinot pakalpojumu pieejamības un izmantošanas iespējas ekonomiskajā darbībā. Tika strādāts arī iedzīvotāju e-prasmju pilnveides jomā.

Tomēr, neskatoties uz sistemātisko plānošanu, pozitīvajiem sasniegumiem un veiktajiem ieguldījumiem, Eiropas Komisijas 2019. gada ziņojums par Latviju secina (Eiropas Komisija, 2019. gada Eiropas pusgads - novērtējums par progresu strukturālo reformu īstenošanā, makroekonomikas nelīdzsvarotības novēršanā un koriģēšanā, un saskaņā ar Regulu (ES) Nr. 1176/2011 veikto padziļināto pārskatu rezultāti, 2019):

- Zems darbaspēka digitālo prasmju līmenis ierobežo digitālo tehnoloģiju izmantošanu uzņēmumos un inovācijas potenciālu.
- Attiecībā uz digitālajām prasmēm Latvijas rādītāji ir zemāki par ES vidējo rādītāju. Pusei iedzīvotāju (52 %) trūkst digitālo pamatprasmju, un atšķirība salīdzinājumā ar citām ES valstīm ir vēl plašāka padziļinātu prasmju jomā (Eiropas Komisija, 2018j). Valsts stratēģijas mērķis ir nodrošināt apmācību informācijas tehnoloģijās, kas ir pielāgota darba tirgus vajadzībām, iesaistīt šajā jomā jauniešus un izstrādāt modernus un interaktīvus mācību procesus. Latvijai būtu vajadzīgi ievērojami ieguldījumi, lai uzlabotu savu iedzīvotāju un darbaspēka digitālās prasmes, ņemot vērā tās ekonomikas un sabiedrības digitālo pārveidi.;
- Digitālā pārveide norit sekmīgi, taču Latvija atpaliiek attiecībā uz digitālo tehnoloģiju integrāciju uzņēmumos. Latvija turpina uzrādīt nevienmērīgus rezultātus digitālās pārveides jomā. Tās stiprākās jomas ir savienojamība, uzņēmējdarbības kultūra un IKT jaunuzņēmumi, kurās tai ir labāki rezultāti nekā ES vidēji.
- Ar IT saistītie pakalpojumi (it īpaši publiskie IT pakalpojumi) 2018. gadā ievērojami uzlabojās. Pēdējo dažu gadu laikā Latvija ir īstenojusi dažādus politikas pasākumus, lai panāktu uzlabojumus jomās ar mēreniem rādītājiem (piem., inovācijas vaučers) un lai nostiprinātu jomas ar spēcīgiem rādītājiem (piemēram, jaunuzņēmumu darbības atbalsta likums).

- Joprojām pastāv problēmas saistībā ar digitālo tehnoloģiju integrāciju, piekļuvi finansējumam un digitālo prasmju piedāvājumu un pieprasījumu.
- Uzņēmumos nodarbinātu pētnieku (FTE) skaits uz vienu tūkstoti ekonomiski aktīvo iedzīvotāju 2016. gadā atbilst vērtībai 0,6, ierindojoties 24. vietā (ES vidējais rādītājs – 3,9). Eiropas Komisija, Digital Transformation Scoreboard, 2018. gads. absolventu mazais un arvien sarūkošais skaits zinātnes, tehnoloģiju, inženierzinātņu un matemātikas (STEM) jomās veicina augsti kvalificētu cilvēkresursu akūtu trūkumu Latvijas pētniecības un inovācijas sistēmā gan pētniecības iestādēs, gan ražošanas nozarē. Demogrāfisko pārmaiņu dēļ šī problēma nākotnē var saasināties.
- Digitālo pakalpojumu integrācija pakāpeniski uzlabojas, taču trūkst kvalificētu IT speciālistu. Uzņēmumi arvien vairāk izmanto mākoņdatošanu un elektronisko informācijas apmaiņu, taču kopumā šo pakalpojumu izmantošana, salīdzinot ar ES vidējiem rādītājiem, ir ierobežota.
- Latvijas uzņēmumi joprojām nepietiekami izmanto preču un pakalpojumu tiešsaistes pārdošanas un iegādes potenciālu, līdz ar to rādītāji ir ievērojami zemāki par ES vidējo attiecībā uz MVU e-komerciju un saistītiem apgrozījuma līmeņiem.
- Digitālo pakalpojumu izmantošana ir plaša, taču digitālo prasmju līmenis joprojām ir problēma. Arvien vairāk Latvijas iedzīvotāju izmanto interneta pakalpojumus, piemēram, interneta banku un e-pārvaldes pakalpojumus. Tomēr iedzīvotāju digitālās prasmes būs jāuzlabo, ja Latvija vēlas gūt labumu, ko dod iekļaujošs darba tirgus, un uzlabot uzņēmumu produktivitāti un digitālo tehnoloģiju integrāciju.

Neskatoties uz grūtībām, publisko pakalpojumu attīstība tika plānota arī turpmāk. NAP 2021-2027, kurš tika apstiprināts Nacionālās attīstības padomē un Ministru kabinetā (attiecīgi 13.02.2020. un 25.02.2020) vēl pirms ārkārtējās situācijas izsludināšanas, paredzēja turpināt un mērķtiecīgi attīstīt digitālo tehnoloģiju izmantošanu, t.sk. nospraužot tādas mērķus kā zināšanu sabiedrības veidošanu, digitālo iespēju izmantošanu publiskajā pārvaldē, tiesiskuma nodrošināšanā, integrētu sociālās un veselības aprūpes pakalpojumu sniegšanu, izmantojot digitalizētas platformas u.c. (Pārresoru koordinācijas centrs, Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam., 2020).

NAP 2021-2027 apstiprinātie uzstādījumi ir iestrādāti VARAM izstrādātajās digitālās transformācijas pamatnostādņēs (VARAM, Digitālās transformācijas pamatnostādnes 2021-2027. gadam. Projekts., 2021), kas sagatavotas saskaņā ar Digitālās Eiropas programmu 2021-2027. gadam, ņemot vērā ES Digitālajā stratēģijā noteiktās digitālās attīstības prioritātes.

04.02.2020. Ministru kabinets apstiprināja VARAM izstrādāto Pakalpojumu vides pilnveides plānu 2020.-2023. gadam, kas, cita starpā, nosaka mērķi - pārvaldes pakalpojumi iedzīvotājiem un uzņēmējiem ir lietotājiem orientēti - proaktīvi, vienlīdz pieejami visai sabiedrībai, atbalstoši un personalizēti, un valsts pārvalde pakalpojumu sniegšanā ir atvērta un efektīva, izmanto mūsdienu tehnoloģiju iespējas un inovatīvus risinājumus, kā arī sadarbojas nacionāli un pāri robežām.

Ņemot vērā iepriekš minēto, jāsecina, ka publisko pakalpojumu digitalizācijas jomā Latvijā ir noticis un notiek rūpīgs un mērķtiecīgs darbs, kas aptver gan politikas plānošanas gan normatīvo aktu izstrādes jomas.

Nepastāv būtiski juridiski šķēršļi digitālo risinājumu izmantošanai publiskajā pārvaldē un civiltiesiskajās attiecībās.

Atpaliek iedzīvotāju un uzņēmēju digitālās prasmes un pieejamo risinājumu pielietojums.

3.2.2. Ārkārtējā situācijas laikā

Pēc ārkārtējās situācijas izsludināšanas krasi palielinājās nepieciešamība digitālajiem risinājumiem attālināta darba veikšanai, kā arī drošības procedūrām šo risinājumu ieviešanā un izmantošanā. Publiskā sektora institūcijām konsultatīvu atbalstu nodrošināja informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV, kura salīdzinoši operatīvi veica populārāko telekonferenču rīku izpēti un sniedza ieteikumus valsts un pašvaldību institūcijām (CERT, 2020).

Līdz ar plašāku elektronisko saziņas līdzekļu lietošanu, aktivizējās dažādi krāpniecības veidi, piemēram, e-pasti kas satur maksājumu pieprasījumus, apsolut rēķinus izsūtīt vēlāk, šantāžas e-pasti gan iedzīvotājiem, gan uzņēmumiem, viltus loterijas u.c. (CERT, Kiberlaikapstākļi (aprīlis), 2020).

Nepieciešamība operatīvi pārorientēties uz darbu attālinātā režīmā parādīja, ka iepriekš nav pievērsta pietiekama uzmanība attālinātā darba tehnoloģiskajam nodrošinājumam. Šos jautājumus iestādēm un uzņēmumiem vajadzēja operatīvi atrisināt līdz ar ārkārtējās situācijas izsludināšanu. Attālinātā darba tehniskais nodrošinājums, tehnisko līdzekļu izmantošanas procedūras un ar to saistītās darbinieku un uzņēmumu vadītāju apmācības būs aktuālas ne tikai ārkārtējās situācijas laikā, bet arī atkopšanās periodā.

3.2.3. Atkopšanās situācijā un jaunajā normālajā situācijā

VARAM izstrādātās Digitālās transformācijas pamatnostādnes, balstoties uz OECD ziņojuma *“Going Digital in a Multilateral World”* (OECD, GOING DIGITAL IN A MULTILATERAL WORLD, 2018) definē 3 hipotētiskus nākotnes attīstības scenārijus, tajos formulējot vīzijas par to, vai nākotnes digitālajā sabiedrībā virsroku ņems sabiedrības daļas pašorganizēšanās, valdību kontrole vai privāto korporāciju ietekme. Tie ir (VARAM, Digitālās transformācijas pamatnostādnes 2021-2027. gadam. Projekts., 2021):

- **#Me2.0 (iChoose)** Cilvēki ir izmantojuši digitālās tehnoloģijas, lai radītu jaunas sociālās kustības un kopienas savu interešu īstenošanai. Šīs kustības ir apstrīdējušas valdību un uzņēmumu dominējošo stāvokli, veidojot spēcīgu trešo pīlāru pasaules varas sistēmā. Kopienas izmantotehnoloģijas, lai risinātu vietējās un globālās problēmas, vienlaikus aizsargājot savu datu piederību. Polarizācija starp sabiedrības grupām un jautājumi par atbildību joprojām rada izaicinājumus.
- **Platform Governments.** Valdības funkcionē, izmantojot ļoti efektīvas tiešsaistes platformas, kas nodrošina ekonomisko apmaiņu un lielāko daļu citu darbību. Lielākā daļa valdību pieder pie politiskiem blokiem ar platformām, kas mijiedarbojas savā starpā, bet ne ar citiem blokiem. Digitālajai infrastruktūrai ir īpaši svarīga loma valstu attīstības un drošības stratēģijās. Valdībukontrole pār lieliem datu apjomiem uzliek tām arī lielu atbildību un rada nepieciešamību pēc līdzsvarotiem pārvaldības un uzraudzības risinājumiem.
- **Corporate Connectors.** Neliels skaits globālo tehnoloģiju uzņēmumu ir vienas pieturas aģentūras katram dzīves aspektam. Ar savu ekonomisko spēku un sabiedrības vajadzību analīzi tehnoloģiju korporācijas ir ieguvušas leģitimitāti ļoti būtiskai lomai globālajā pārvaldībā. Daudzas jomas, par kuriem iepriekš bija atbildīgas valdības, tagad ir korporāciju rokās.

Šie uzstādījumi ir spēkā standarta jeb normālajā situācijā, kas pastāvēja līdz ārkārtējā stāvokļa izsludināšanai. Globālā pandēmija radīja nepieciešamību paskatīties uz šiem visaugstākā līmeņa plānošanas dokumentiem no cita skata punkta.

Ja normālā situācijā Nacionālās attīstības plāns nosaka stratēģiskos mērķus, prioritātes un uzdevumus valsts attīstībai nākamajiem septiņiem gadiem, lai panāktu Latvijas un ikviena iedzīvotāja izaugsmi un labklājības pieaugumu (Pārresoru koordinācijas centrs, Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam., 2020), tad pandēmija liek detalizētāk izvērtēt situāciju visas valsts, sabiedrības, ekonomikas un pakalpojumu noturības kontekstā.

Pēdējās desmitgadēs uzmanība tika pievērsta galvenokārt ekonomisko un sociālo sistēmu darbības un pārvaldības efektivitātei, kas noveda pie sazarotas savstarpēji atkarīgas sistēmas izveidošanās (piemēram, starptautiskas piegāžu ķēdes), kas ir neaizsargātas pret pēkšņiem traucējumiem. Kompleksās sistēmās vienmēr pastāvēs pretruna starp efektivitāti un noturību - spēju paredzēt, absorbēt, atgūties no triecieniem un piemēroties tiem (OECD, A systemic resilience approach to dealing with Covid-19 and future shocks, 2020).

Digitālo risinājumu ieviešana ir viens no līdzekļiem, lai pārvarētu Covid-19 izraisīto krīžu sekas un virzītos tālāk, ņemot vērā gūtās mācības.

Pandēmijas radīto seku novēršanā tiek realizētas daudzas un dažādas atbalsta programmas. Praktiski visās attīstītajās pasaules valstīs notiek visdažādākās darbības krīžu seku mazināšanā. Nepastāv viens optimālais risinājums, kuru varētu izmantot kā labāko praksi. Turklāt, pasākumi krīžu seku mazināšanai nepieciešami nekavējoties. Tas nozīmē, ka lielā ātrumā tiek veidoti paralēli risinājumi, kas balstās katras valsts kultūrā, tiesību aktos, ekonomiskajā un sociālajā sistēmā. Domājot par jebkuras sistēmas darbību ilgtermiņā, ir skaidrs, ka būtu lietderīga realizēto pasākumu padziļināta analīze (tas nozīmē nepieciešama nepieciešamo datu uzkrāšana), lai izstrādātu labākos scenārijus un rīcības plānus sistēmu noturības paaugstināšanai nākotnē.

Paralēli tam turpinās jau uzsākto programmu realizācija, sekojot NAP nospraustajiem mērķiem. Tas nozīmē, ka pasākumi krīzes seku novēršanai tiks realizēti vienlaikus ar plānotajiem pasākumiem digitalizācijas jomā.

4. Jaunu IKT izmantošanas potenciāls uzņēmējdarbībā

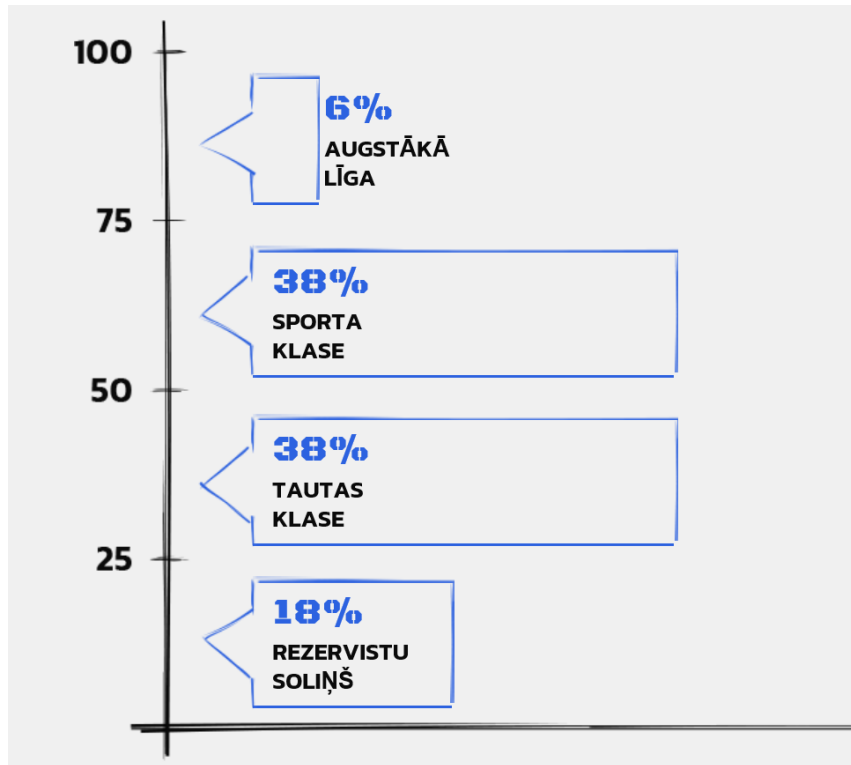
4.1. Uzņēmumu digitālā brieduma līmenis

Lai apzinātu IKT tehnoloģijas izvērtējuma iespējas krīzes un pēckrīzes stāvoklī, ir nozīmīgi identificēt uzņēmumu digitālā brieduma līmeni.

Uzņēmumu digitālā brieduma līmenis raksturo uzņēmuma esošās digitālās spējas (Aguiar, Boguea Gomes, Rupino da Cunha, & Mira da Silva, 2019). Tipiski digitālā brieduma līmeņa noteikšanai tiek izmantota 5 līmeņu skala atbilstoši CMMI rekomendācijām. Šajā dokumentā ir izmantota gudralatvija.lv esošā skala, kas nosaka 4 digitālā brieduma līmeņus:

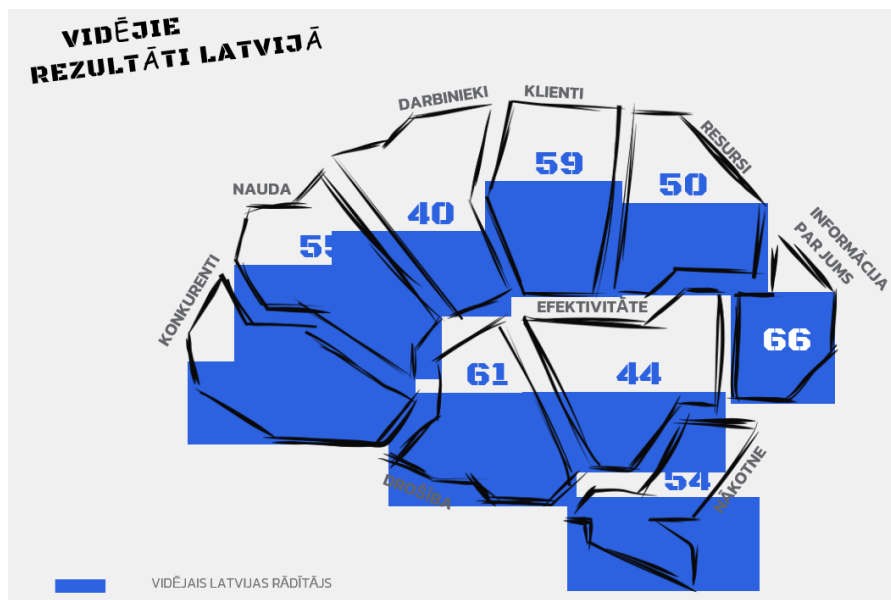
- 1. līmenis – rezervistu soliņš;
- 2. līmenis – tautas klase;
- 3. līmenis – sporta klase;
- 4. līmenis – augstākā līga.

Latvijas uzņēmumu lielākais īpatsvars atrodas 2. un 3. līmenī (Ilustrācija 11).



Ilustrācija 11 Latvijas uzņēmumu digitalizācijas līmenis (LIKTA, 2020)

Latvijas vidējie rezultāti (Ilustrācija 12) rāda, ka uzņēmumi tehnoloģijas aktīvi izmanto informācijas par sevi izplatīšanai (sociālie tīkli, tīmekļa vietnes u.c.), pakalpojumu sniegšanai klientiem, kā arī informācijas drošības nodrošināšanai. Mazāk tehnoloģijas tiek izmantotas efektivitātes uzlabošanai (procesu automatizācija u.c.), darbinieku un resursu pārvaldībai. No minētā secināms, ka attālinātā darba nodrošināšanā ārkārtas situācijās uzņēmēji saskaras ar izaicinājumiem un informācijas drošības nodrošināšanā ir vieta uzlabojumiem.



Ilustrācija 12 Latvijas uzņēmumu digitalizācijas līmenis (LIKTA, 2020)

4.2. Aktuālās digitalizācijas tendences uzņēmējdarbībā

4.2.1. Tendencu kopsavilkums

Digitalizācija ir viens no aktuālākajām uzņēmējdarbības attīstības virzieniem. To virza ne vien organizāciju vēlme radīt jaunus produktus, pakalpojumus un palielināt to pievienoto vērtību, bet arī sociālekonomiskās, kulturālas pārmaiņas un ārējās vides ietekme. Digitalizācijas tendences raksturo aktuālās metodes un tehnoloģijas, kas plaši tiek izmantotas uzņēmumos. Digitalizācijā vērojamas kopīgas tehnoloģiju izmantošanas tendences (t.i., “horizontālās” tendences), bet atkarībā no nozares mainās specifiskie tehnoloģiju lietošanas gadījumi (t.i., “vertikālās tendences”). Piemēram, “horizontālās” tendences “augstas veiktspējas datošanas izmantošana produktos, procesos un pakalpojumos” viens lietošanas gadījums jeb “vertikālā” tendence enerģētikas nozarē ir “augstas veiktspējas tehnoloģiju izmantošana energoturbīnu optimizēšanai”.

Nozaru būtiskākās kopīgās digitalizācijas tendences ir iedalāmas trīs grupās:

1. **Datu analītika un pārvaldība** – plaša datu koplietošana un analīze ikdienas procesu īstenošanā (t.sk., procesu izpildes kvalitātes novērošana un koriģēšana reāllaikā vai tuvu tam);
2. **Biznesa procesu analīze un automatizācija** – procesu apzināšana un racionalizācija, biznesa procesu izpilde ar minimālu cilvēku iesaistīšanos (t.sk., resursu pārvaldība kapacitātes un noslodzes paaugstināšanas nolūkos un cilvēkresursu izmantošana augstas pievienotās vērtības aktivitātēm);
3. **Inovāciju tehnoloģiju izmantošana procesos, produktos, pakalpojumos** – tradicionālie darbības veidi un produkti tiek papildināti ar digitālajām tehnoloģijām, piem., valkājamās ierīces.

Dokumentā ir veikts tendenču salīdzinājums dažādās situācijās. Tendencu izmantošana ir apskatīta nozaru neatkarīgos jeb “horizontālajos” lietošanas gadījumos – drošs attālināts darbs un droši pamatservisi un nozaru specifiskajos jeb “vertikālajos” lietošanas gadījumos – droši biznesa servisi (pasažieru pārvadājumi).

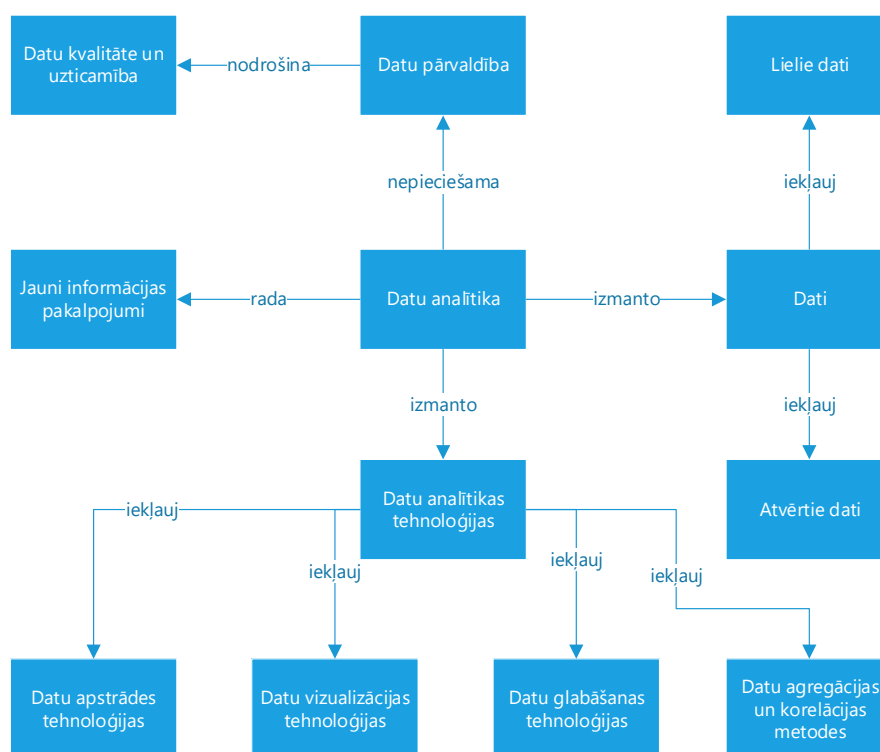
Salīdzināšanas rezultātā ir iegūti secinājumi par IKT izmantošanu, saistību starp dažādo situāciju kopīgajām un atšķirīgajām iezīmēm, kā arī sagatavoti priekšlikumi IKT izmantošanai uzņēmējdarbībā (11.1. nodaļa) un priekšlikumi valsts atbalstam un intervencei (11.2.nodaļa).

4.2.1.1. Datu analītika un datu pārvaldība

Datu analītika un pārvaldība nozīmē plašu datu koplietošanu un analīzi ikdienas procesu īstenošanā, kas iekļauj dažādus savstarpēji saistītus komponentus – datus, datu analītikas tehnoloģijas, datu pārvaldību, datu kvalitāti un uzticamību un jaunus informācijas pakalpojumus (Ilustrācija 13).

Dati un to analītika tipiski tiek izmantota uzņēmumu darbības analīzei, prognozēšanai, lēmumu pieņemšanai, uzņēmumu attīstības plānošanai, kā arī jaunu informācijas pakalpojumu izveidei (Salkin, Oner, Ustundag, & Cevikcan, 2018), (Aguilar, Roland, & Twardowski, 2018), (Michel A. & Michielin, 2020). Būtisks datu analītikas izmantošanas gadījums ir kvalitātes vadība. Tas ir procesu izpildes kvalitātes novērošana un koriģēšana reāllaikā vai tuvu tam, kas iekļauj dažādus uzņēmējdarbības kvalitātes vadības veidus - uzņēmuma darbības novērtēšana, kļūdu un defektu identificēšana, procesu darbības monitoring (Fisseler,

Kemény, & Reiners, 2016). Ar tehnoloģiju palīdzību uzņēmumi uzlabo produktu un pakalpojumu kvalitāti (Albukhitan, 2020).



Ilustrācija 13 Datu analītikas un datu pārvaldības komponenti

Drošs attālināts darbs

Drošam attālinātam darbam datu analītika var tikt izmantota uzņēmumu darbības novērtēšanai, procesu darbības monitoringam, darbinieka pienākumu kvalitatīvas un efektīvas izpildes novērtēšanai, drošības risku analīzei, efektīvas komunikācijas novērtēšanai, darbinieku motivācijas novērtēšanai. Datu analītikai var tikt izmantoti datu analītikas risinājumi, ko var papildināt ar mākslīgā intelekta risinājumiem (piemēram, darbinieku emociju analīzei). Datu analītikai primāri izmantojami uzņēmuma uzkrātie dati (klientu atsauksmes, kavētās dienas, darbinieka izpildītie uzdevumi, komunikācijai patērētais laiks u.c.), kas papildināmi ar atvērtajiem datiem (risku un ievainojamību saraksti u.c.) un lielajiem datiem (iekārtu un tīkla notikumi u.c.). Procesu darbības monitoringus papildus var aptvert līdzekļu izmantošanas/darbības (*asset performance*) pārvaldību.

Tehnoloģiju izmantošana droša attālināta lietošanas darba gadījumā būs līdzīga dažādās situācijās – pirmskrīzes, krīzes, atkopšanās un jaunajā normālajā situācijā. Bet palielināsies tehnoloģiju izmantošanas intensitāte, piemēram, normālā situācijā darbinieku emocijas motivācijas līmeņa noteikšanai primāri iespējams analizēt klātienē tikšanās laikā, savukārt krīzes situācijā (strādājot tikai no mājām), tam var tikt izmantotas tehnoloģijas.

Droši pamatservisi

Drošu pamatservisu nodrošināšanai datu analītika var tikt izmantota drošības incidentu analīzei un pieslēgumu noturības analīzei. Datu analītikai var tikt izmantoti datu analītikas

risinājumi, kas var tikt papildināti ar mākslīgā intelekta risinājumiem (piemēram, potenciālo drošības incidentu identificēšanai). Datu analītikai var tikt izmantoti uzņēmuma uzkrātie dati (auditācijas pieraksti par aizdomīgām lietotāju darbībām un netipisku uzvedību, incidentu skaits un novēršanas laiks u.c.), lielle dati (tīkla notikumu dati – aizdomīgi DNS izsaukumi) un atvērtie dati (ievainojamību un risku saraksti, uzticamu IKT pakalpojumu sniedzēju saraksti).

Tehnoloģiju izmantošana drošu pamatservisu lietošanas gadījumā dažādās situācijās neatšķirsies, bet krīzes situācijās, palielinoties attālinātam darbam, datu analītikai ir kritiska nozīme (pamatservisu neesamība var pilnībā paralizēt uzņēmumu darbību).

Droši biznesa servisi

Biznesa servisu (pasažieru pārvadājumi) nodrošināšanai normālā situācijā datu analītika var tikt izmantota maršrutu optimizācijai (pasažieru plūsmas, braukšanas manevri, kalendārs, laks u.c.), sabiedriskā transporta pienākšanas laika prognozēšanai (braukšanas apstākļi, kalendārs, laiks u.c.), CO₂ izmešu un ietekmes uz gaisa kvalitāti novērtēšanai (degviela, CO₂ dati, gaisa kvalitātes dati u.c.). Datu analītikai var tikt izmantoti uzņēmuma uzkrātie dati (degvielas izlietojums, pasažieru skaits u.c.), lielle dati (GPS dati transporta atklāšanas vietas noteikšanai) un atvērtie dati (gaisa kvalitātes dati, laikapstākļu dati).

Biznesa servisi (pasažieru pārvadājumi) krīzes situācijā būtiski mainās – droša pakalpojuma sniegšanai ir nepieciešams ievērot virkni ar jaunām prasībām, no kurām būtiskākās ir distancēšanās prasības (pasažieriem ir jānodrošina iespējas ievērot distanci no citiem pasažieriem gan transportlīdzeklī, gan pieturvietā), kā arī transportlīdzekļa dezinfekcijas prasības, kas var atstāt ietekmi uz to kustības grafiku. Krīzes situācijā datu analītika var tikt izmantota pasažieru plūsmas monitoringam un brauciena pārvaldībai. Datu analītikai var tikt izmantoti uzņēmuma uzkrātie dati (vēsturiskie transportlīdzekļa kustības dati), lielle dati (GPS dati transporta līdzekļa atrašanās vietas noteikšanai), atvērtie dati (laikapstākļu dati, satiksmes dati). Atvērto ģeotelpisko datu integrēšanai digitālo pakalpojumu sniegšanā nepieciešama būtiska to priekšapstrāde, līdz ar to būtu noderīgas vadlīnijas atvērto datu izmantošanai un apstrādei pakalpojumu sniegšanā (zināšanas, kas konceptualizējamas šablona formā).

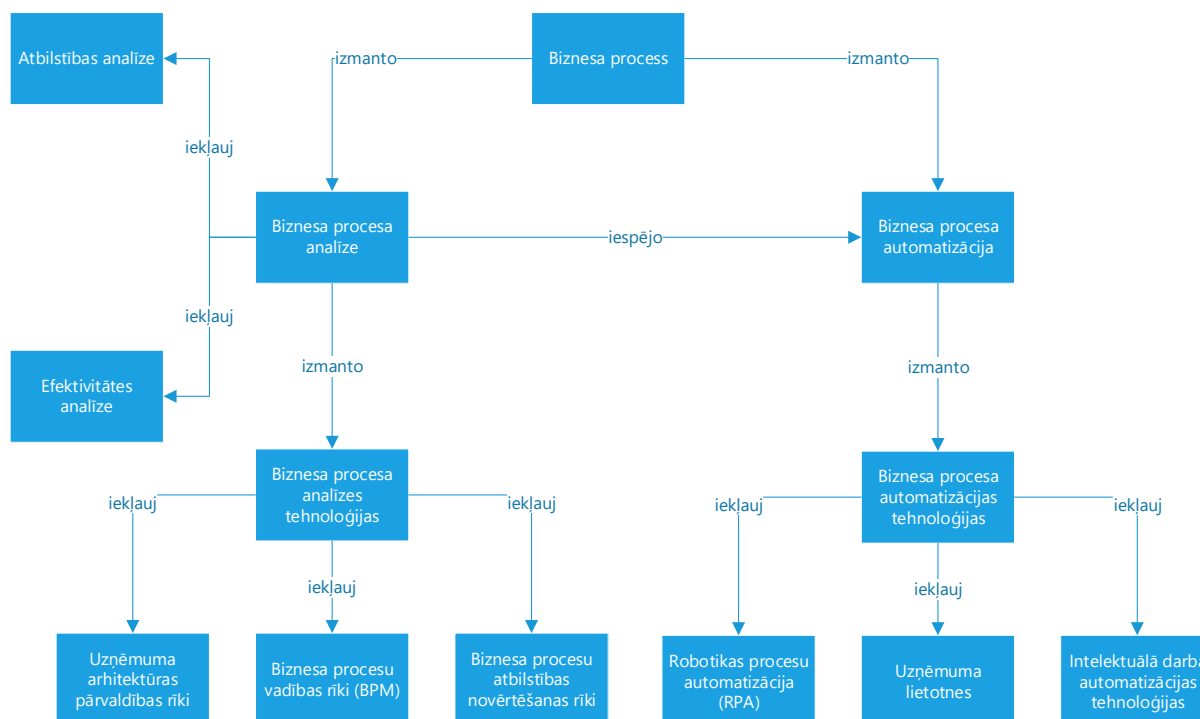
4.2.1.2. Biznesa procesu analīze un automatizācija

Biznesa procesu analīze un automatizācija iekļauj vairākus savstarpēji saistītus komponentus – biznesa process, biznesa procesa analīze un analīzes tehnoloģijas, biznesa procesa automatizācija un automatizācijas tehnoloģijas (Ilustrācija 14).

Biznesa procesu analīze ir procesu apzināšana un racionalizācija, kā arī atbilstības nodrošināšana regulējošajām prasībām. Uzņēmējdarbības digitalizācijai un uzņēmuma darbības novērtēšanai nozīmīga loma ir biznesa procesu analīzei. Tipiski biznesa procesi tiek analizēti ar mērķi veikt to efektīvizāciju (piemēram, identificēt aktivitātes, kas nesniedz pievienoto vērtību), novērtēt procesu atbilstību normatīvajam regulējumam, kā arī veikt procesu pārveidi, t.sk., automatizējot procesus (Li, Dong, Shang, & Zhao, 2018), (Kotamarthi, Wang, Grossmann, Sheng, & Indrakanti, 2015).

Biznesa procesu automatizācija ir biznesa procesu izpilde ar minimālu cilvēku iesaistīšanos, kas iekļauj pamatdarbības procesu automatizāciju, atbalsta procesu automatizāciju un biznesa procesu pielāgošana standartprogrammatūrai. Uzņēmumu biznesa procesu automatizācija, izmantojot tehnoloģiju (roboti, lietotnes, mākslīgais intelekts u.c.)

sniegtās iespējas joprojām ir aktuāla tendence uzņēmējdarbībā (Albukhitan, 2020), (Goncarovs, 2019). Automatizācija aptver gan rutīnas darbu automatizāciju, piemēram, dokumentu reģistrācija, sanāksmju laiku ievade kalendārā, gan arī intelektuālo darbu automatizāciju, piemēram, personalizēta ārstēšanās plāna izveide, uzņēmuma vadība (Schrettenbrunner, 2020). Automatizēti tiek gan atbalsta (Xiao, 2020), gan pamatdarbības, t.sk., tehnoloģiskie procesi (Plyatsuk, u.c., 2020).



Ilustrācija 14 Biznesa procesu analīzes un automatizācijas komponenti

Drošs attālināts darbs

Droša attālināta darba īstenošanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai. Lai uzņēmums varētu plānot biznesa nepārtrauktību un veikt procesu un servisu simulēšanu dažādās situācijās, uzņēmumiem ir būtiski apzināt un aprakstīt biznesa kritiskās spējas, biznesa procesus, kā arī veikt to sasaisti ar informācijas un tehnoloģiju resursiem un servisiem. Biznesa procesu aprakstīšanai un analīzei var tikt izmantoti Biznesa procesu vadības (BPM) rīki, uzņēmuma arhitektūras rīki, kā arī pārvaldības – risku – atbilstības (GRC) rīki.

Tehnoloģijas var tikt izmantotas biznesa procesu automatizācijai (attālinātā darba kontekstā - atbalsta procesu automatizācijai). Būtiskākie attālināto darbu atbalstošie automatizējamie procesi:

1. finanšu pārvaldība un iepirkumu pārvaldība (nepieciešamās tehnikas iegāde attālinātā darba nodrošināšanai u.c.);
2. cilvēkresursu pārvaldība (darba laika uzskaitē, darbinieku motivācijas monitorings, apmācību plānošanas un īstenošana);
3. darbu pārvaldība (darbu plānošana, darbu izpildes kontrole u.c.);

4. komunikācijas pārvaldība (komunikācijas pieejamības nodrošināšana, notifikāciju pārvaldība u.c.);
5. IT pārvaldība (IT risku pārvaldība, atbilstības pārvaldība u.c.).

Procesu automatizācijai iespējams izmantot dažādas uzņēmumu lietotnes, piemēram, uzņēmumu resursu pārvaldības sistēmas, finanšu vadības sistēmas, darba laika uzskaites sistēmas, incidentu pārvaldības sistēmas, e-apmācību sistēmas, komunikācijas pārvaldības rīki, aptauju rīki, informācijas vietnes, kā arī mākslīgā intelekta risinājumi intelektuālā darba automatizācijai.

Liela daļa atbalsta procesu automatizācijas lietotņu ir pieejamas standatrisinājumu un “sistēma-kā-pakalpojums” (SaaS) veidā. Rutīnas darbību automatizācijai iespējams izmantot arī robotikas procesu automatizācijas (RPA) risinājumus, piemēram, komunikācijā patērētā laika uzskaitē.

Tehnoloģiju izmantošana droša attālināta lietošanas darba gadījumā būs līdzīga dažādās situācijās – pirmskrīzes, krīzes, atkopšanās un jaunajā normālajā situācijā.

Droši pamatservisi

Drošu pamatservisu nodrošināšanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai (analogi kā droša attālinātā darba gadījumā).

Tehnoloģijas var tikt izmantotas biznesa procesu automatizācijai (drošu pamatservisu kontekstā - atbalsta procesu automatizācijai). Būtiskākie drošus pamatservisus atbalstošie automatizējamie procesi:

- IT drošības pārvaldība, tajā skaitā:
 - IT risku pārvaldība (risku reģistrēšana, risku novērtēšana, risku vadība u.c.);
 - incidentu pārvaldība (monitorings, incidentu ziņošana, incidentu izmeklēšana u.c.).
- komunikācijas pārvaldība (darbinieku informēšana par informācijas drošību, IT riskiem, IT drošības notikumu un incidentu ziņošana u.c.);
- cilvēkresursu pārvaldība (IT drošības apmācību plānošanas un īstenošana).

Atbalsta procesu automatizācijai iespējams izmantot dažādas informācijas sistēmas, piemēram, pārvaldības-risku-atbilstības (GRC) sistēmas, incidentu pārvaldības sistēmas, risku pārvaldības sistēmas, e-apmācību sistēmas, komunikācijas pārvaldības rīkus, informācijas vietnes, monitoringa sistēmas, SIEM sistēmas kā arī mākslīgā intelekta risinājumus.

Liela daļa atbalsta procesu automatizācijas lietotņu ir pieejamas standatrisinājumu un “sistēma-kā-pakalpojums” (SaaS) veidā.

Tehnoloģiju izmantošana drošu pamatservisu lietošanas darba gadījumā būs līdzīga dažādās situācijās – pirmskrīzes, krīzes, atkopšanās un jaunajā normālajā situācijā.

Droši biznesa servisi

Drošu biznesa servisu (pasažieru pārvadājumi) īstenošanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai (analogi kā droša attālinātā darba gadījumā).

Tehnoloģijas var tikt izmantotas biznesa procesu automatizācijai (drošu biznesa servisu kontekstā – pamatdarbības un atbalsta procesu automatizācijai).

Būtiskākie drošus biznesa servisos (pasažieru pārvadājumi) atbalstošie automatizējamie procesi normālā situācijā:

- maršrutu plānošana;
- resursu pārvaldība (autoparks, šoferi) un izlietojuma monitorings un kontrole;
- satiksmes vadība (maršrutu plānošana un optimizācija, ietekmes uz vidi samazināšana u.c.);
- biznesa nepātrauktības plānošana.

Krīzes situācijā nozīmīgākais papildus automatizējamais process ir brauciena pārvaldība, kura ietvaros tiek analizēta brauciena informācija (pasažieru skaits, transporta kustība u.c.), sniegtas rekomendācijas šoferam tālākai rīcībai (neuzņemt jaunus pasažierus u.c.) un apziņoti pasažieri par gaidāmā vai aktuālā brauciena informāciju (transportlīdzeklis ir pilns un neuzņems pasažierus, gaidāma transportlīdzekļa aizkavēšanās u.c.).

Procesu automatizācijai var tikt izmantotas uzņēmumu resursu pārvaldības sistēmas, transporta vadības sistēmas, maršrutēšanas rīki, optimizācijas sistēmas un mākslīgais intelekts. Procesu automatizācijas iespējošanai nepieciešamas GNNS tehnoloģijas, datu pārraidei rekomendēts izmantot 5G tehnoloģijas.

4.2.1.3. Inovatīvo tehnoloģiju izmantošana procesos, produktos un pakalpojumos

Inovatīvo tehnoloģiju izmantošana procesos, produktos un pakalpojumos nozīmē tradicionālo uzņēmumu darbības veidu un produktu papildināšana ar digitālajām tehnoloģijām, piem., valkājām ierīcēm. Uzņēmējdarbībā biežāk izmantojamās inovatīvās tehnoloģijas ir (Culot, Orzes, Sartor, & Nassimbeni, 2020), (Salkin, Oner, Ustundag, & Cevikcan, 2018), (Markvarte, 2020), (Vandvik & Brandt, 2020), (Derksen & Weber, 2017), (Laibach, Börner, & Bröring, 2019): mākslīgais intelekts, roboti, lietu internets un viedās ekosistēmas, blokķēdes, 5G tehnoloģijas, papildinātā un virtuālā realitāte un augstas veiktspējas datošana (HCP) (Ilustrācija 15).

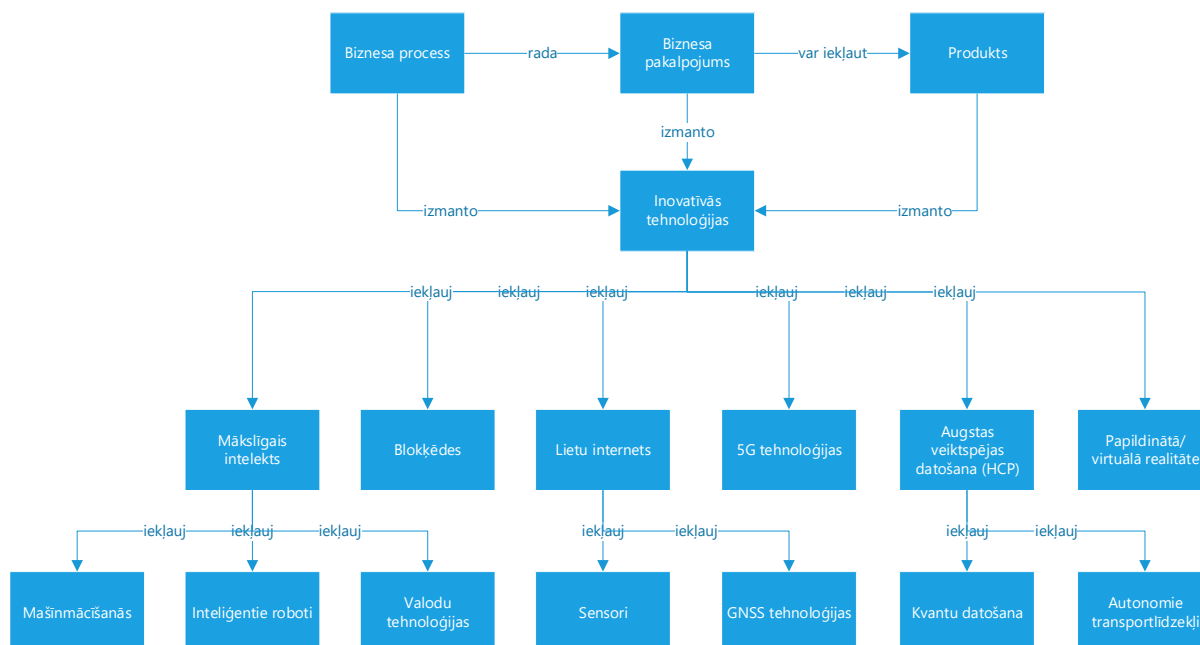
Eiropas līmenī īpaši izceltas tiek mākslīgā intelekta un augstas veiktspējas datošanas tehnoloģijas (Eiropas Komisija, Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, 2018).

Ar augstas veiktspējas datošanas palīdzību tiek risinātas problēmas dažādās jomās, no kurām būtiskākās ir personalizētā medicīna, bioinženierija, laika prognozēšana un klimata pārmaiņas, jaunu materiālu un zāļu atklāšana, naftas un gāzes iegulu izpēte, jaunu lidmašīnu un automobiļu projektēšana un viedpilsētas (Eiropas Komisija, HPC - BEST USE EXAMPLES, 2018). Zemes zinātnes un klimata politikas jomās augstas veiktspējas datošana tiek izmantota, lai precīzāk prognozētu laika apstākļus, paredzētu lielas kataklizmas un pētīt okeānu uzvedību. Drošas, tīras un efektīva enerģijas jomā augstas veiktspējas datošana tiek izmantota atjaunojamās enerģijas parku un augstas veiktspējas fotoelementu izveidē, energoturbīnu optimizēšanā. Veselības, demogrāfisko pārmaiņu un labklājības jomā augstas veiktspējas datošana tiek izmantota personalizētai medicīnai un precīzijas medicīnai, kas apstrādā informāciju par cilvēka gēniem, olbaltumiem un vidi, nolūkā novērst, diagnosticēt un ārstēt slimības. Tāpat medicīnā augstas veiktspējas datošanu izmanto biomolekulārajā pētniecībā biomolekulu un olbaltumu dinamikas izmeklēšanā cilvēka šūnās. Pārtikas

nodrošinājuma, ilgtspējīgas lauksaimniecības, jūras zinātniskajā un tehniskajā pētniecībā un bioekonomikā augstas veiktspējas datošana tiek izmantota ilgtspējīgākas lauksaimniecības attīstīšanā, pārtikas ražošanas optimizēšanā, ilgtspējas faktoru analizēšanā un sērgu novērošanā, slimību kontrolē un pesticīdu novērošanā. Kiberdrošība un kiberaizsardzības jomās augstas veiktspējas datošana tiek izmantota sarežģītu šifrēšanas tehnoloģiju izstrādei, kiberuzbrukumu analīzei un novēršanai, efektīvas tiesu ekspertīzes veikšanai, kā arī veicot kodoliekārtu modelēšanu. Viedas, ekoloģiskas un integrēta pilsētplānošanas jomā augstas veiktspējas datošana tiek izmantota viedo pilsētu izveidē un attīstībā (transporta infrastruktūras reāllaika datu analītikai u.c.), kā arī autonomu transportlīdzekļu (transportlīdzekļi bez vadītāja) izveidei.

Savukārt, mākslīgais intelekts uzlabo produktus, procesus un darbības modeļus visās tautsaimniecības nozarēs. Eiropas Komisija rosina pieeju mākslīgā intelekta attīstības centrā nolikt cilvēku un izmantot mākslīgā intelekta tehnoloģijas pasaules lielāko problēmu risināšanā, piemēram, slimību ārstēšanai, dabas katastrofu prognozēšanai, klimata pārmaiņām, transporta drošības uzlabošanai, noziedzības apkarošanai un kiberdrošības uzlabošanai (Eiropas Komisija, Koordinētais mākslīgā intelekta plāns, 2018). Mākslīgā intelekta tehnoloģijas arī kļūst par vienu no galvenajiem līdzekļiem, ar kuriem uzņēmumi visā pasaulē uzlabo klientu apkalpošanu, piedāvā individualizētus pakalpojumus un ceļ darba efektivitāti. Mākslīgais intelekts palīdz automatizēt biznesa procesus jaunā kvalitātē (VARAM, 2019). Tipiskākie mākslīgā intelekta lietojumi ir lēmumu pieņemšanas automatizācija un atbalsts, mašīntulkošana un valodu tehnoloģijas, virtuālie asistenti, datu analītika, lielo datu masīvu analīze un uz tās balstīta prognozēšana, attēlu atpazīšana un datorredze, mašīnmācīšanās un robotika.

Inovatīvās tehnoloģijas tiek kombinētas ar mērķi palielināt produktu un pakalpojumu pievienoto vērtību klientiem un paaugstināt uzņēmumu darbības efektivitāti. Digitālo inovāciju radīšanai tiek kombinētas organizatoriskās inovācijas (Maldaner, u.c., 2020). Viedās ierīces tiek kombinētas ar padomdevēju sistēmām, piemēram, medicīnā, lai palīdzētu pacientam sasniegt atveseļošanās mērķus. Ražošanas līnijas un produkti tiek aprīkoti ar sensoriem, kas sniedz plašu analītisko informāciju, kas tiek izmantota produktu uzlabošanai un jaunu pakalpojumu radīšanai. Lietošanas datu un saistīto servisu apvienošana produktu platformās ļauj dinamiski noteikt pakalpojumu cenas un pielāgot citus produkta un pakalpojuma parametrus.



Ilustrācija 15 Uzņēmējdarbībā biežāk izmantotās inovatīvās tehnoloģijas

Drošs attālināts darbs

Drošam attālinātam darbam būtiskākās izmantojamās inovatīvās tehnoloģijas ir: mākslīgais intelekts un 5G tehnoloģijas.

Mākslīgais intelekts var tikt izmantots lielākajā daļā droša attālinātā darba procesos, piemēram, papildinot vienkāršotu datu analītiku ar mākslīgā intelekta risinājumiem. Tāpat mākslīgā intelekta risinājumi izmantojami informācijas apmaiņas veicināšanai. Tipiskākie uzņēmumu procesi, kur izmantojams mākslīgais intelekts ir:

- IT pārvaldība (IT risku pārvaldība, atbilstības pārvaldība u.c.);
- darbinieku motivācijas līmeņa analīzei;
- komunikācijas pārvaldība, piemēram, komunikācijas pieejamības nodrošināšana var tikt izmantoti inteligētie aģenti un čātboti;
- uzņēmuma darbības novērtēšanai.

Drošam attālinātā darbam nozīmīgas ir arī 5G tehnoloģijas, darbam un mācībām pārejot attālinātā režīmā, 4G tīkla tehnoloģijas ne vienmēr ir pietiekamas nepārtraukta darba nodrošināšanai.

Tehnoloģiju izmantošana droša attālinātā lietošanas darba gadījumā būs līdzīga dažādās situācijās – pirmskrīzes, krīzes, atkopšanās un jaunajā normālajā situācijā. Bet palielināsies tehnoloģiju izmantošanas intensitāte, piemēram, normālā situācijā darbinieku emocijas motivācijas līmeņa noteikšanai primāri iespējams analizēt klātienes tikšanās laikā, savukārt krīzes situācijā (strādājot tikai no mājām), tam var tikt izmantotas tehnoloģijas, t.sk., mākslīgais intelekts.

Droši pamatservisi

Drošu pamatservisu nodrošināšanai būtiskākās izmantojamās inovatīvās tehnoloģijas ir: mākslīgais intelekts, 5G tehnoloģijas un augstas veiktspējas datošanas (HCP) tehnoloģijas. Tehnoloģijas primāri izmantojamas kiberdrošības nodrošināšanai (piemēram, potenciālo drošības incidentu identificēšanai).

Droši biznesa servisi

Drošu biznesa servisu nodrošināšanai būtiskākās izmantojamās inovatīvās tehnoloģijas ir: lietu internets, mākslīgais internets, 5G tehnoloģijas un HCP tehnoloģijas.

Normālā situācijā lietu internets izmantojams maršrutēšanai, viedajai satiksmes vadībai un transporta pienākšanas laika prognozēšanai. Lietu internets apvieno sensoru un GNNS datus (transporta kustība, satiksme u.c.) ar datu analīzes un pārvaldības lietotnēm (piemēram, maršrutēšanas lietotnēm), veidojot dažādu objektu tīklus. Objektu tīkli ir papildināmi ar mākslīgā intelekta risinājumiem, kas analizējot dažāda veida datus (dati no sensoriem, GNSS, konteksta dati, atvērtie dati u.c.) izveido rekomendācijas. Datu pārraidei būtiskas ir 5G tehnoloģijas. Dažādo datu (īpaši lielo datu) efektīvai apstrādei izmantojamas HCP tehnoloģijas.

Krīzes situācijā izmantojamās inovatīvās tehnoloģijas ir analogas, bet atšķiras to izmantošanas gadījumi, krīzes situācijās aktuāls ir pasažieru plūsmas monitorings un brauciena pārvaldība. Abiem lietošanas gadījumiem rekomendēts izmantot lietu internetu dažādo objektu datu apvienošanai (sensori, GNNS u.c), mākslīgo internetu rekomendāciju sistēmām (piemēram, rekomendācijas transportlīdzekļa vadītājam par veicamajām darbībām, piemēram, maršruta maiņa), 5G tehnoloģijas datu pārraidei un HCP tehnoloģijas datu apstrādei.

4.2.2. Tendencu salīdzinošā analīze

Normālā situācijā uzņēmumi palielina tehnoloģiju izmantošanu produktos, procesos un pakalpojumos, pakāpeniski palielinot digitālā brieduma līmeni. Tehnoloģiju attīstības un uzņēmējdarbības digitalizācija ietekme rodas sociālekonomiskās un kulturālās pārmaiņas. Paaugstinās klientu gaidas no pakalpojumiem – klienti sagaida, ka vairums pakalpojumi ir pieejami elektroniski, 24/7 režīmā. Mainās procesijas, darbinieku lomas un pienākumi. Darbinieku digitālo kompetenču nozīme pieaug (Gigova, Valeva, & Nikolova-Alexieva, 2019).

Krīzes situācijās IKT tehnoloģijas tiek plaši izmantotas gan biznesa nepārtrauktības nodrošināšanai, gan krīzes seku likvidācijai un normālas darbības atjaunošanā. Salīdzinot ar normālo situāciju, IKT izmantošanas tendences ir tādas pašas, bet IKT izmantošanas intensitāte palielinās. Digitālie kanāli ārkārtas situācijās paliek primārie vai pat vienīgie. Mainās arī tehnoloģiju izmantošanas gadījumi, piemēram, normatīvo aktu izmaiņu ietekmē (piemēram, distancēšanās prasības rada jaunus tehnoloģiju izmantošanas gadījumus pasažieru pārvadājumu nodrošināšanā).

Atkošanās un jaunajā normālajā situācijā tehnoloģijas tiks izmantotas līdzīgā apjomā kā krīzes situācijā. Uzņēmumi un publiskās pārvaldes iestādes lielākoties ir pārorientējuši darbu no klātienē uz attālināto darbu, ir izveidoti jauni digitāli pakalpojumi un digitālie kanāli. Paredzams, ka atkopšanās un jaunajā normālajā situācijā daļa klātienē darba un pakalpojumu atgriezīsies, bet tomēr attālinātais darbs un digitālie pakalpojumi un kanāli paliks kā primārie.

4.3. Digitalizāciju kavējošie un veicinošie faktori

4.3.1. Kavējošie faktori

Krīzes un pēckrīzes apstākļos biežākie IKT izmantošanas kavējošie faktori ir saistīti nevis ar tehnoloģisko risinājumu nepieejamību, bet gan ar organizatoriskiem aspektiem – uzņēmējiem pietrūkst zināšanas un spējas risinājumu ieviešanai un drošai izmantošanai. Esošais normatīvais regulējums vairums gadījumu ir dažādi interpretējams. Visbiežāk ar digitalizācijas izaicinājumiem saskaras tieši mazo un vidējo uzņēmumu segments (OECD, Going Digital in Latvia, 2020).

Tipiskākie IKT izmantošanas krīzes un pēckrīzes situācijās kavējošie faktori ir šādi:

1. Trūkst nepieciešamo spēju (kompetence, kapacitāte u.c.), grūtības piesaistīt ekspertus. Gandrīz puse no visiem Latvijas uzņēmumiem, kas vēlas pieņemt darbā Informācijas komunikācijas tehnoloģijas (IKT) speciālistus, ziņo par grūtībām aizpildīt vakances (VARAM, Digitālās transformācijas pamatnostādnes 2021-2027. gadam. Projekts., 2021);
2. Finansējuma nepietiekamība – IKT risinājumu ieviešanai nepieciešamas salīdzinoši lielas kapitālās izmaksas, kas īpaši MVU segmentā ir būtiski kavējošs faktors;
3. Normatīvais regulējums ir formāls un dažādi interpretējams. MVU segmentam bieži ir grūtības gan ar digitalizāciju, gan informācijas drošības un personas datu aizsardzības aspektu nodrošināšanu, jo pietrūkst normatīvo aktu skaidrojumu (piemēram, elektronisku dokumentu aprīte, personas datu aizsardzības nodrošināšanas aspekti u.c.);
4. Organizācijas kultūra, nevēlēšanās ieviest pārmaiņas;
5. Neuzticība digitālajām tehnoloģijām un šaubas par to izmantošanas stabilitāti, uzticamību un drošību;
6. Digitālā transformācija uzņēmumos bieži tiek skatīta no tehnoloģiju un tehnikas inovāciju skatupunkta, nevis no sociālo inovāciju jeb darbības pārveides skatupunkta (biznesa procesi, cilvēki), kas ir pretēji digitalizācijas pamatidejai un nesekmē pilnīgu digitalizācijas ieguvumu realizāciju.

4.3.2. Veicinošie faktori

Krīzes un pēckrīzes apstākļos būtiskākie IKT izmantošanu veicinošie apstākļi ir ārējās vides ietekme, kā arī normatīvais regulējums.

Tipiskākie IKT izmantošanas krīzes un pēckrīzes situācijās veicinošie faktori ir šādi:

1. Normatīvais regulējums, kas vērsts uz IKT pastiprinātu izmantošanu, piemēram, saņemot publiskos pakalpojumus (piemēram, augstāka pakalpojuma maksa vai ilgāks pakalpojuma rezultāta gaidīšanas laiks klātienēs kanālu izmantošanas gadījumā);
2. Valsts pakalpojumu sistēmu obligātas izmantošanas noteikšana;
3. Sociālekonomiskās un kulturālās pārmaiņas. Ar katru gadu aug klientu prasības un gaidas no pakalpojumiem. Tiem jābūt pieejamiem attālināti, 24/7, neizejot no savas atrašanās vietas. Aug arī prasības uzņēmējdarbībā izmantojamajām tehnoloģijām, piemēram, vērojams patērētāju pieprasījums pēc arvien "gudrākiem" virtuālajiem asistentiem.

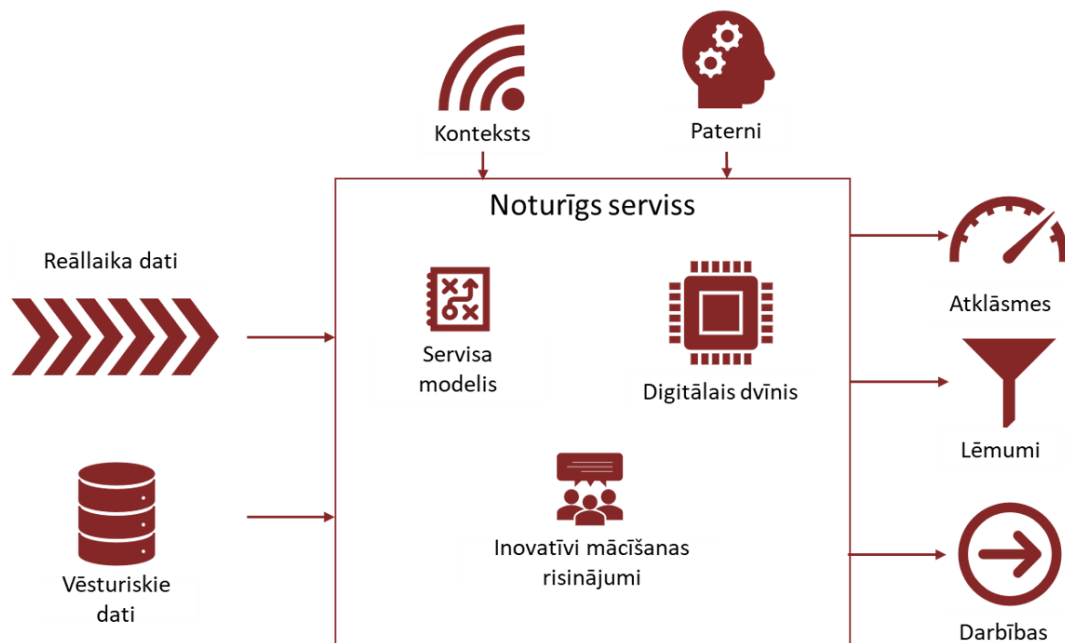
5. Servisu drošības un noturības nodrošināšanas paņēmieni

COVID-19 krīze izgaismoja esošo digitālo servisu iespējas un mainīja to darbību, kā arī radīja jaunus servissus ar nezināmu uzticamības pakāpi. Būtiski nodrošināt servisu drošību un noturību. To var sasniegt, veidojot un darbinot servissus, kuriem noturība ir viena no to pamatiezīmēm. Lai to sasniegtu, ARTSS projekts postulē, ka noturīgu servisu veidošana ir organizāciju spēja, kas var tikt sasniegta savstarpēji sadarbojoties un apmainoties ar zināšanām organizāciju un ieinteresēto pušu ekosistēmā.

Noturīgu un drošu servisu pamatā ir (Ilustrācija 16):

- digitālā dvīņa izmantošana, kas ļauj simulēt un kontrolēt servisa darbību krīzes situācijās;
- inovatīvi e-apmācības risinājumi, kas servisu lietotājiem sniedz servisu izmantošanas prasmes;
- zināšanu apmaiņa šablonu veidā ātrai zināšanu uzkrāšanai par krīzes seku pārvarēšanas risinājumiem.

ARTSS pieeja ietver metodi un tehnoloģisko risinājumu digitālo pakalpojumu dinamiskai pielāgošanai krīzes situācijām. Metodes pamatā ir servisu spēju virzīta izstrādes metodoloģija, un tā tiks izvērtēta četros uz programmu attiecināmos lietošanas gadījumos. Projektā arī tiks sagatavotas rīcībpolitikas rekomendācijas un izvērtējumi par drošu telemedicīnas, biznesa un e-apmācības servisu nodrošināšanu



Ilustrācija 16 ARTSS pieeja

Metodes pilns apraksts sniegts Projekta dokumentā “WP1: Noturīgu servisu izstrādes un darbināšanas metode”.

Projekta gaitā pētīti četri lietošanas gadījumi – drošs attālināts darbs, droši telemedicīnas servisi, droši biznesa servisi (transporta pārvaldījumi) un droši pamatservisi (droša tīkla pārvaldība). Zināšanas par ārkārtas situācijā izmantotajām tehnoloģijām šablonu veidā ir apkopotas zināšanu repozitorijā - <https://artss.rtu.lv/repository/web/lv>

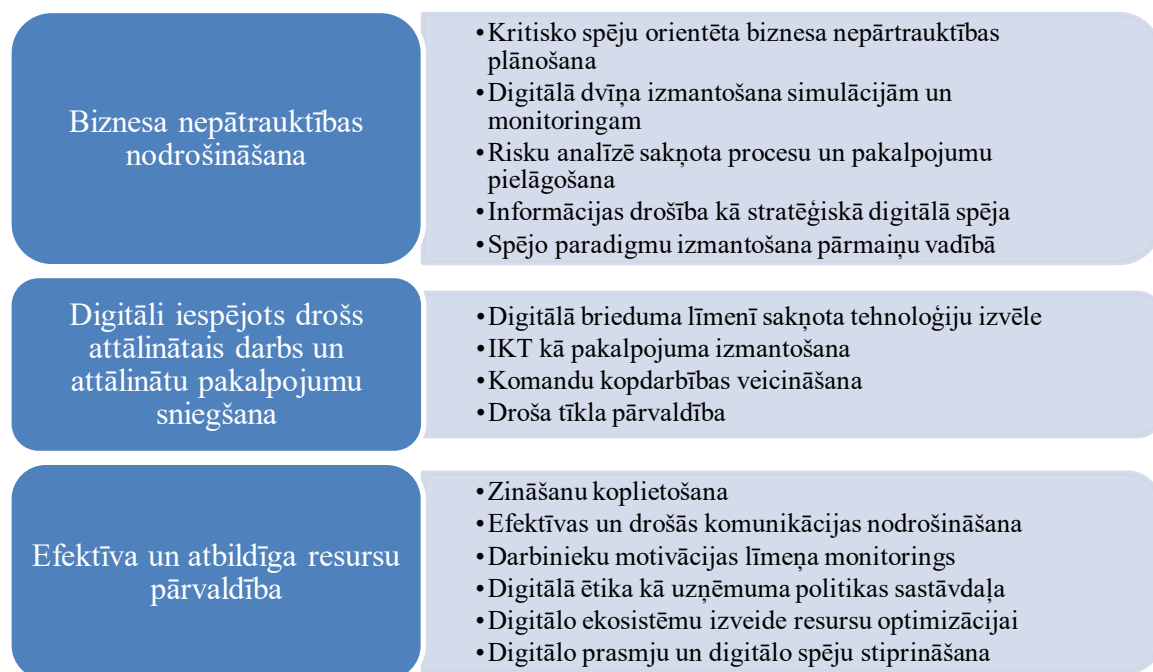
6. Priekšlikumi

Nodaļā sniegti priekšlikumi par būtiskākajiem veicamajiem organizatoriskajiem pasākumiem drošu un noturīgu servisu nodrošināšanai, tehnoloģijām un to pielietojumiem, kas nodrošina uzņēmējdarbības procesu nepārtrauktību, kā arī rekomendācijas nepieciešamajam valsts atbalstam vai valsts intervencei tehnoloģiju plašākai izmantošanai uzņēmējdarbībā.

6.1. Priekšlikumi uzņēmējiem

Priekšlikumi uzņēmējiem aptver trīs galvenos virzienus (Ilustrācija 17):

4. Biznesa nepārtrauktības nodrošināšana – priekšlikumi preventīvajiem un uzraudzības pasākumiem, kas veicami biznesa nepārtrauktības nodrošināšanai ārkārtas situācijās;
5. Digitāli iespējots drošs un nepārtraukts darbs – priekšlikumi tehnoloģiju izmantošanai attālinātā darba organizācijai ārkārtas situācijā (tehnoloģiju un rīku izmantošana, digitālas darba vietas, izklīdētu komandu kopdarbība u.c.);
6. Efektīva un atbildīga resursu pārvaldība – priekšlikumi uzņēmumu resursu efektīvai pārvaldībai ārkārtas situācijā (zināšanas, cilvēkresursi u.c.).



Ilustrācija 17 Priekšlikumi uzņēmējiem drošu un noturīgu servisu nodrošināšanai

6.1.1. Biznesa nepārtrauktības nodrošināšana

6.1.1.1. Kritisko spēju orientēta biznesa nepārtrauktības plānošana

Biznesa nepārtrauktības plānošanas mērķis ir nodrošināt biznesa kritisko spēju un pakārtoto biznesa procesu nepārtrauktību ārkārtas situācijās. Biznesa nepārtrauktības plānošanu rekomendēts sākt ar biznesa ietekmes analīzi, kas ir pamats biznesa nepārtrauktības un IS nepārtrauktības un darbības atjaunošanas plānošanai. Biznesa ietekmes analīzes gaitā tiek analizēta «graujošu» notikumu finansiālā un operatīvā ietekme uz organizācijas darbību

(biznesa spējām, biznesa procesiem u.c.). Finansiālā ietekme ir attiecināma uz monetāriem zaudējumiem, piemēram, neiegūtā pārdošanas peļņa, neiegūtais finansējums u.c.. Darbības ietekme ir attiecināma uz nemonetāriem zaudējumiem, piemēram, reputācijas zudums, klientu apmierinātības samazināšanās, konkurētspējas samazināšanās. Pēc biznesa ietekmes analīzes, tiek veikta biznesa nepārtrauktības plānošana, kas ietver šādas galvenās aktivitātes:

1. Stratēģisko spēju identificēšana - apskatīt un noteikt spējas, kas nepieciešamas uzņēmuma mērķu izpildei mainīgos kontekstuālos apstākļos;
2. Alternatīvo procesu izstrāde (kā uzņēmums darbosies ārkārtas situācijās);
3. Noturīga un droša servisa definēšana - definēt spēju un procesu īstenošanai nepieciešamos programmatūras servisu, galveno vērību pievēršot servisiem, kas būtiski ietekmē kopējo spējas noturīgumu un drošību;
4. Darbības atjaunošanas stratēģijas izstrāde (biznesa procesu atjaunošana u.c.);
5. Biznesa nepārtrauktības plāna izstrāde
6. IS darbības nepārtrauktības un atjaunošanas plāna izstrāde.

Biznesa nepārtrauktības plānošanai rekomendēts izmantot spēju modeļus, ko iespējams lietot kā pamatu spējas darbības pārvaldības sistēmas izstrādei un digitālā dvīņa izstrādei (skatīt piemēru 1.pielikumā).

6.1.1.2. Digitālā dvīņa izmantošana ārkārtas situāciju un pakalpojumu dinamiskai simulēšanai un monitoringam

Biznesa nepārtrauktības plānošanai un nodrošināšanai rekomendēts izmantot uzņēmuma digitālo dvīni. Dvīnis izmantojams gan alternatīvo procesu modelēšanai biznesa nepārtrauktības plānošanai, gan servisa drošības un noturības rādītāju pastāvīgai pārraudzībai biznesa nepārtrauktības nodrošināšanai. Digitālais dvīnis izmanto reāllaika datus par servisu nodrošināšanu (tos attēlo mērāmie atribūti), novērtē potenciālos servisa nodrošināšanas apdraudējumus un rekomendē pielāgojumus, kuri būtu jāizmanto servisa darbības un spējas īstenošanas uzlabošanai. Digitālais dvīnis atspoguļos tos servisu tīkla aspektus, kas ir visnozīmīgākie drošības un noturības nodrošināšanai. Digitālā dvīņa izveidei priekšnosacījums ir biznesa ietekmes analīze, kuras laikā tiek identificēti biznesa kritiskās spējas un mērķi, kas tiek izteikti spēju modeļa veidā. Galvenās digitālā dvīņa izveides aktivitātes ir:

1. Definēt digitālā dvīņa tvērumu - kuriem spēju nodrošinājumiem servisiem konstruē digitālo dvīni;
2. Identificēt digitālā dvīņa izmantošanai atbilstošos mērķus - spēju modelī nosaka mērķus, kuru sasniegšanas novērtēšanai tiks izmantots digitālais dvīnis;
3. Identificēt digitālā dvīņa reāllaika ieejas datus - spēju modelī nosaku, kuri mērāmie atribūti vai konteksta elementi tiks izmantoti digitālajā dvīnī;
4. Identificēt digitālā dvīņa reāllaika iedarbes - nosaka, kurus spējas pielāgojumus izsauks digitālajā dvīnī pieņemtie lēmumi;
5. Projektēt rādītāju paneli;
6. Projektēt simulācijas modeli - atbilstoši simulācijas modeļu izstrādes metodoloģijai izveido simulācijas modelis, kuru eksperimentēšanai un lēmumpieņemšanai izmantos digitālais dvīnis.;
7. Izveidot eksperimentu plānu;
8. Projektēt lēmumpieņemšanas modeli - kā atbilstoši simulācijas rezultātiem izvēlēties reāllaika iedarbes;

9. Ģenerēt digitālā dvīņa apvalku - digitālā dvīņa vizualizācijas ģenerēšana;
10. Ģenerēt digitālā dvīņa sagatavi mērķa izstrādes vidē.

Digitālā dvīņa piemērs sniegts 4.pielikumā.

6.1.1.3. Risku analīzē saknota procesu un pakalpojumu pielāgojumu plānošana

Katra uzņēmuma līmenī ir jāveic risku novērtēšana, izpildot šādas secīgas darbības:

- Risku identificēšana un novērtēšana;
- Iespējamo pielāgojumu apzināšana;
- Risku, pielāgojumu un risku mazināšanas pasākumu novērtēšana (skaitliskā izteiksmē);
- Lēmumu pieņemšana par risku mazināšanas pasākumiem atbilstoši risku novērtējumam.

Izvērtējot riskus ieteicams ņemt vērā ne tikai paša uzņēmuma riskus, bet arī kontekstu – ārējos apstākļus, kuri ietekmē uzņēmuma darbību: valsts rīcībpolitikas, pieņemtos lēmumus, infrastruktūras un darbaspēka pieejamību utt.

Detalizētu risku novērtēšanas algoritmu skat.2.3. nodaļā.

6.1.1.4. Informācijas drošība kā stratēģiskā digitālā spēja

Informācijas drošība ir uzņēmuma un privātpersonu datu un digitālās identitātes aizsargāšana. Informācijas drošība un īpaši kiberdrošība ir aktuāla tēma jau vairākus gadu desmitus. Kiberuzbrukumu veidi katru gadu mainās, līdz ar to ir nozīmīgi nodrošināt atbilstošu fizisko un loģisko aizsardzību. Uzņēmumiem rekomendēts informācijas drošību definēt kā stratēģisko digitālo spēju un pievērst tai uzmanību, definējot to stratēģiskajos mērķus. Mērķu definēšanai iespējams izmantot spēju un servisu modeli, kas attēlo aspektus, kas ir svarīgi servisa drošības un noturības nodrošināšanai (skatīt 1.pielikumu).

6.1.1.5. Spējo paradigmu izmantošana pārmaiņu vadībā

Lai spētu operatīvi reaģēt uz ārkārtas situāciju izraisītajām izmaiņām, uzņēmējdarbībā rekomendēts izmantot spējās paradigmas, piemēram, Lean, Agile. Paradigmas ir fokusētas uz kultūras maiņu, nodrošinot efektīvu komandu sadarbību, vērtības radīšanu un izvairīšanos no liekā patēriņa (waste).

6.1.2. Digitāli iespējots drošs attālinātais darbs un attālināta pakalpojumu sniegšana

6.1.2.1. Digitālā brieduma līmenī saknota tehnoloģiju izvēle

Tehnoloģijas ir nozīmīgas drošu un noturīgu servisu nodrošināšanai, tomēr nereti uzņēmumi izvēlas ieviest tehnoloģijas, kas nav atbilstošas uzņēmumu spējām tās faktiski izmantot un ieviest (t.i., tās nav atbilstošas uzņēmuma digitālā brieduma līmenim). Šādu tehnoloģiju izmantošana nesniedz uzņēmumiem plānoto investīciju atdevi, kā arī nereti netiek sasniegts tehnoloģijas ieviešanas mērķis (piemēram, no nepareizas vai nepilnīgas tehnoloģiju izmantošanas). Uzņēmumiem rekomendēts tehnoloģijas izvēlēties, vērtējot to esošo brieduma līmeni (piemēram, mikrouzņēmums datu analīzei var izmantot Excel datnes un pēc nepieciešamības vienkāršotus datu vizualizācijas rīkus, savukārt – lielajam uzņēmumam piemērotākas var būt datu noliktavas un biznesa analītikas tehnoloģijas).

Būtiskākās rekomendējamās tehnoloģijas drošam attālinātam darbam

Datu analītikas tehnoloģijas (biznesa inteligences rīki, datu noliktavas, datu vizualizācijas rīki, datu straumēšanas tehnoloģijas, datu ezeri u.c.). Datu analītika ir plaši izmantojama uzņēmuma darbības monitoringam un kvalitātes kontrolei (darbinieka pienākumu kvalitatīva un efektīva izpilde, komunikācijas efektivitāte, darbinieku motivācija u.c.), kas ir īpaši svarīgs attālinātā darba gadījumā, kad darbu izpilde nav tik pārskatāma.

Biznesa procesu analīzes un automatizācijas tehnoloģijas. Droša attālināta darba īstenošanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai, kā arī procesu automatizācijai.

Biznesa procesu analīzes tehnoloģijas (Biznesa procesu vadības (BPM) rīki, uzņēmuma arhitektūras rīki, Pārvaldības – risku- atbilstības (GRC) rīki u.c.) izmantojami, lai uzņēmums varētu plānot biznesa nepārtrauktību un veikt procesu un servisu simulēšanu dažādās situācijās, uzņēmumiem ir būtiski apzināt un aprakstīt biznesa kritiskās spējas, biznesa procesus, kā arī veikt to sasaisti ar informācijas un tehnoloģiju resursiem un servisiem.

Biznesa procesu automatizācijas tehnoloģijas (RPA, uzņēmuma lietotnes, intelektuālā darba automatizācijas risinājumi u.c.), izmantojamas procesu vai aktivitāšu automatizācijai, samazinot manuālā darba apjomu. Efektīva attālināta darba nodrošināšanai iespējams automatizēt lielu daļu no “atbalsta” procesiem, no kuriem būtiskākie ir:

- finanšu pārvaldība un iepirkumu pārvaldība (nepieciešamās tehnikas iegāde attālinātā darba nodrošināšanai u.c.);
- cilvēkresursu pārvaldība (darba laika uzskaitē, darbinieku motivācijas monitoringa, apmācību plānošanas un īstenošana);
- darbu pārvaldība (darbu plānošana, darbu izpildes kontrole u.c.);
- komunikācijas pārvaldība (komunikācijas pieejamības nodrošināšana, notifikāciju pārvaldība u.c.);
- IT pārvaldība (IT risku pārvaldība, atbilstības pārvaldība u.c.).

Inovatīvās tehnoloģijas procesu un pakalpojumu pilnveidei. Drošam attālinātam darbam būtiskākās izmantojamās inovatīvās tehnoloģijas ir: mākslīgais intelekts un 5G tehnoloģijas.

Mākslīgais intelekts var tikt izmantots lielākajā daļā droša attālinātā darba procesos, piemēram, papildinot datu analītiku ar mākslīgā intelekta risinājumiem. Tāpat mākslīgā intelekta risinājumi izmantojami informācijas apmaiņas veicināšanai. Tipiskākie uzņēmumu procesi, kur izmantojams mākslīgais intelekts ir:

- IT pārvaldība (IT risku pārvaldība, atbilstības pārvaldība u.c.);
- darbinieku motivācijas līmeņa analīzei;
- komunikācijas pārvaldība, piemēram, komunikācijas pieejamības nodrošināšana var tikt izmantoti inteligēntie aģenti un čātboti;
- uzņēmuma darbības novērtēšanai.

Drošam attālinātam darbam nozīmīgas ir arī 5G tehnoloģijas, darbam un mācībām pārejot attālinātā režīmā, 4G tīkla tehnoloģijas ne vienmēr ir pietiekamas nepārtraukta darba nodrošināšanai.

Būtiskākās rekomendējamās tehnoloģijas drošu pamatservisu nodrošināšanai

Datu analītikas tehnoloģijas (biznesa inteligences rīki, datu noliktavas, datu vizualizācijas rīki, datu straumēšanas tehnoloģijas, datu ezeri u.c.). Drošu pamatservisu nodrošināšanai datu analītika var tikt izmantota drošības incidentu analīzei un pieslēgumu noturības analīzei. Datu analītikai izmantojamie datu analītikas risinājumi var tikt papildināti ar mākslīgā intelekta risinājumiem (piemēram, potenciālo drošības incidentu identificēšanai).

Biznesa procesu analīzes tehnoloģijas (Biznesa procesu vadības (BPM) rīki, uzņēmuma arhitektūras rīki, Pārvaldības – risku - atbildības (GRC) rīki u.c.) un **biznesa procesu automatizācijas tehnoloģijas** (pārvaldības-risku-atbildības (GRC) sistēmas, incidentu pārvaldības sistēmas, risku pārvaldības sistēmas, e-apmācību sistēmas, komunikācijas pārvaldības rīki, informācijas vietnes, monitoringa sistēmas, SIEM sistēmas u.c.). Drošu pamatservisu nodrošināšanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai (analogi kā droša attālinātā darba gadījumā), kā arī biznesa procesu automatizācijai. Būtiskākie drošus pamatservisus atbalstošie automatizējamie procesi:

- IT drošības pārvaldība, tajā skaitā:
 - IT risku pārvaldība (risku reģistrēšana, risku novērtēšana, risku vadība u.c.);
 - incidentu pārvaldība (monitorings, incidentu ziņošana, incidentu izmeklēšana u.c.).
- komunikācijas pārvaldība (darbinieku informēšana par informācijas drošību, IT riskiem, IT drošības notikumu un incidentu ziņošana u.c.);
- cilvēkresursu pārvaldība (IT drošības apmācību plānošanas un īstenošana).

Procesu automatizācijai iespējams izmantot dažādas informācijas sistēmas, piemēram, pārvaldības-risku-atbildības (GRC) sistēmas, incidentu pārvaldības sistēmas, risku pārvaldības sistēmas, e-apmācību sistēmas, komunikācijas pārvaldības rīkus, informācijas vietnes, monitoringa sistēmas, SIEM sistēmas, kā arī mākslīgā intelekta risinājumus.

Drošu pamatservisu nodrošināšanai būtiskākās izmantojamās inovatīvās tehnoloģijas ir: mākslīgais intelekts, 5G tehnoloģijas un augstas veiktspējas datu apstrādes (HCP) tehnoloģijas. Tehnoloģijas primāri izmantojamas kibernetikas drošības nodrošināšanai (piemēram, potenciālo drošības incidentu identificēšanai).

Būtiskākās rekomendējamās tehnoloģijas drošu biznesa servisu nodrošināšanai

Datu analītikas tehnoloģijas (biznesa inteligences rīki, datu noliktavas, datu vizualizācijas rīki, datu straumēšanas tehnoloģijas, datu ezeri u.c.). Biznesa servisu (pasažieru pārvadājumi) nodrošināšanai normālā situācijā datu analītika var tikt izmantota maršrutu optimizācijai (pasažieru plūsmas, braukšanas manevri, kalendārs, laks u.c.), sabiedriskā transporta pienākšanas laika prognozēšanai (braukšanas apstākļi, kalendārs, laiks u.c.), CO2 izmešu un ietekmes uz gaisa kvalitāti novērtēšanai (degviela, CO2 dati, gaisa kvalitātes dati u.c.). Biznesa servisi (pasažieru pārvadājumi) krīzes situācijā būtiski mainās – droša pakalpojuma sniegšanai ir nepieciešams ievērot virkni ar jaunām prasībām, no kurām būtiskākās ir distancēšanās prasības (pasažieriem ir jānodrošina iespējas ievērot distanci no citiem pasažieriem gan transportlīdzeklī, gan pieturvietā), kā arī transportlīdzekļa dezinfekcijas prasības, kas var atstāt ietekmi uz to kustības grafiku. Krīzes situācijā datu analītika var tikt izmantota pasažieru plūsmas monitoringam un brauciena pārvaldībai.

Biznesa procesu analīzes tehnoloģijas (Biznesa procesu vadības (BPM) rīki, uzņēmuma arhitektūras rīki, Pārvaldības – risku- atbilstības (GRC) rīki u.c.) un biznesa procesu automatizācijas tehnoloģijas (uzņēmumu resursu pārvaldības sistēmas, transporta vadības sistēmas, maršrutēšanas rīki, optimizācijas sistēmas u.c.). Drošu biznesa servisu nodrošināšanai tehnoloģijas var tikt izmantotas biznesa procesu identificēšanai, aprakstīšanai un novērtēšanai (analogi kā droša attālinātā darba gadījumā), kā arī biznesa procesu automatizācijai. Būtiskākie drošus biznesa servisos (pasažieru pārvadājumi) atbalstošie automatizējamie procesi normālā situācijā:

- maršrutu plānošana;
- resursu pārvaldība (autoparks, šoferi) un izlietojuma monitorings un kontrole;
- satiksmes vadība (maršrutu plānošana un optimizācija, ietekmes uz vidi samazināšana u.c.);
- biznesa nepātrauktības plānošana.

Krīzes situācijā nozīmīgākais papildus automatizējams process ir brauciena pārvaldība, kura ietvaros tiek analizēta brauciena informācija (pasažieru skaits, transporta kustība u.c.), sniegtas rekomendācijas šoferam tālākai rīcībai (neuzņemt jaunus pasažierus u.c.) un apziņoti pasažieri par gaidāmā vai aktuālā brauciena informāciju (transportlīdzeklis ir pilns un neuzņems pasažierus, gaidāma transportlīdzekļa aizkavēšanās u.c.).

Drošu biznesa servisu nodrošināšanai būtiskākās izmantojamās inovatīvās tehnoloģijas ir: lietu internets, mākslīgais internets, 5G tehnoloģijas un HCP tehnoloģijas. Normālā situācijā lietu internets izmantojams maršrutēšanai, viedajai satiksmes vadībai un transporta pienākšanas laika prognozēšanai. Krīzes situācijā izmantojamās inovatīvās tehnoloģijas ir analogas, bet atšķiras to izmantošanas gadījumi, krīzes situācijās aktuāls ir pasažieru plūsmas monitorings un brauciena pārvaldība. Abiem lietošanas gadījumiem **rekomendēts izmantot lietu internetu dažādo objektu datu apvienošanai (sensori, GNSS u.c), mākslīgo internetu rekomendāciju sistēmām (piemēram, rekomendācijas transportlīdzekļa vadītājam par veicamajām darbībām, piemēram, maršruta maiņa), 5G tehnoloģijas datu pārraidei un HCP tehnoloģijas datu apstrādei.**

Konkrētu tehnoloģiju izmantošanas rekomendācijas, kas atkarīgas no uzņēmuma brieduma līmeņa, sniegtas 5.pielikumā.

Būtiski ir nodrošināt tehnoloģiju izmantošanai nepieciešamo infrastruktūru (t.sk., lietotāju gala iekārtas, tīklu, izvietošanas infrastruktūru). Tehnoloģijas rekomendēts izmantot pakalpojuma veidā (skatīt 10.1.2.2.).

6.1.2.2. IKT kā pakalpojuma izmantošana

Industrijā arvien vairāk tiek izmantoti mākoņdatošanas risinājumi, kas ietver gan lietotnes kā pakalpojumus, gan infrastruktūru kā pakalpojumus. Populāras ir mākoņplatformas (piemēram, *Microsoft Azure*, *Amazon Web Services*), kur iespējams izvietot uzņēmumu lietotnes un izmantot infrastruktūru kā pakalpojumu (IaaS) (Albukhitan, 2020). Mākoņplatformu izmantošana sniedz uzņēmumiem vairākas priekšrocības, tostarp, samazinātas ar infrastruktūras uzturēšanu saistītās izmaksas, mērogojamības iespējas.

Tehnoloģiju izmantošanas gadījumi un apjoms dažādās situācijās (normālā, ārkārtas u.c.) mainās. Uzņēmumiem ir jābūt gataviem ātri pielāgoties izmaiņām, t.sk., mainīt resursu izmantošanas apjomu, resursiem jābūt mērogojamiem. Līdz ar to rekomendēts IKT izmantot pakalpojumu veidā, piemēram, realizējot “Programmatūra kā pakalpojums” (SaaS),

“Infrastruktūra kā pakalpojums” (IaaS) vai “Platforma kā pakalpojums” (PaaS) IKT resursu izmantošanas formas.

6.1.2.3. Komandu kopdarbības veicināšana attālinātajā darbā

Attālinātais darbs rada jauna veida darba vietu nepieciešamību. Nozīmīgs ir ne vien tehnoloģiskais nodrošinājums, bet arī kopdarbības rīku pieejamība komandas darbam. Attālinātai komandu kopdarbībai rekomendēts izmantot šādas rīku kategorijas:

- Komunikācijas rīki (piemēram, MS Teams, Slack, ZOOM) – komunikācijas rīki ir kritiski attālinātajā darbā, tie uzlabo komunikācijas ātrumu un efektivitāti. Komunikāciju ir svarīgi fiksēt, lai tā būtu pieejama visiem (arī tiem, kas reālā sarunā nav klāt), kā arī lai būtu pieejama pilna komunikācijas vēsture un ērta meklēšana tajā.
- Kopdarbības rīki (piemēram, MIRO) - kopsadarības rīki ļauj komandām efektīvi kopsadarboties ar mērķi nodrošināt ideju apmaiņu, kopradi un uzlabot sniegumu. Tipisks rīku piemērs ir digitālās kopsadarības tāfeles, kas ļauj komandām kopsadarboties, vizualizējot darba uzdevumus, problēmas, idejas un radot risinājumus
- Informācijas vietnes (piemēram, MS SharePoint, Confluence) – attālinātajā darbā tipiski palēninās informācijas plūsmas starp uzņēmumu un darbiniekiem un darbinieku starpā, lai veicinātu informācijas apmaiņu var tikt izmantotas informācijas vietnes. Informācijas vietnes bieži tiek realizētas “Wiki” formā, ļaujot organizācijas dalībniekiem veidot un pārskatīt informatīvas lapas, rediģēt to saturu un pievienot jaunas lapas. Informācijas vietnēs uzņēmums var glabāt visu svarīgo un darbiniekiem pieejamo informāciju par uzņēmumu, projektiem utt., glabāt datnes, dokumentus, veidnes un citu noderīgu informāciju.
- Darbu plānošanas rīki (piemēram, Trello) – darbu plānošanai un izpildes pārskatam rekomendēts izmantot darbu plānošanas rīkus, piemēram, vizualizējot komandu darbus Kanban dēļos. Tipiski šāda pieeja tiek izmantota IT nozares uzņēmumos un projektos, bet to iespējams pārņemt arī citās nozarēs.

Rīki iedalāmi komerciālos rīkos (to izmantošanai nepieciešamas licences) un brīvprogrammatūras rīkos (tos iespējams izmantot bez maksas). Lielai daļai komerciālo rīku ir pieejama bezmaksas versija, kas iekļauj ierobežotu funkcionalitāti (piemēram, ierobežots lietotāju skaits).

Rekomendācijas un piemēri komandas kopdarbību veicinošajiem rīkiem iekļautas 2.pielikumā.

6.1.2.4. Droši pamatservisi jeb droša tīkla pārvaldība

Pamatservisi jeb tīkla servisi nodrošina citu digitālo pakalpojumu darbību un drošu tīklošanu. Tā kā pandēmijas seku dēļ liela daļa ekonomikas un mācību notiek tiešsaistē, ļaunprātīgas darbības datortīklā būtu jānosaka pēc iespējas ātrāk, jo drošības incidentu rezultātā uzņēmumos var iestāties pilnīgs darbības pārtraukums. Drošu un noturīgu pamatservisu nodrošināšanai rekomendēts īstenot drošības incidentu analīzi un tīkla noturības monitoringu.

Drošības incidentu analīze uzņēmumos ir ierasts process, tomēr pārsvarā tas tiek realizēts tad, kad incidents jau ir iestājies (īpaši MVU segmentā). Rekomendētā pieeja iekļauj tīkla notikumu analīzi ar mērķi identificēt incidentus pirms to iestāšanās. Analīzei izmantojamas datu analītikas tehnoloģijas, lielie dati un atvērtie dati (skatīt 4.2.1.1. nodaļu), kā arī mākslīgā intelekta un mašīnmācīšanās tehnoloģijas (skatīt 4.2.1.3. nodaļu). Drošības incidentu analīzei rekomendēts analizēt IT sistēmu un infrastruktūras notikumu datus

(auditācijas pieraksti par dažāda veida notikumiem, piemēram, netipiskām lietotāju darbībām, ārējiem pieslēgumiem) un ārējos lielos datus (ievainojamību, incidentu saraksti). Ar mākslīgā intelekta palīdzību rekomendēts identificēt potenciālos draudus. Potenciālie draudi tiek identificēti, pamatojoties uz uzkrātajām zināšanām par draudu raksturiezīmēm, kas var tikt apkopotas no dažādiem avotiem, piemēram, vēsturiskie uzņēmuma dati, ārējie apdraudējumu saraksti, uzticamu pakalpojumu sniedzēju saraksti u.c.. Pēc draudu identificēšanas automatizēti rekomendēts noteikt un realizēt tālākās darbības (iekārtu atslēgšana, paziņojumi u.c.). Drošības incidentu rekomendējamās pieejas apraksts sniegts 1.pielikumā.

Tīkla noturības monitoringam rekomendēts analizēt tīkla pārtraukuma datus, kas var tikt iegūti no tīkla datu analīzes (faktiskie pārtraukumi) un no lietotāju ziņoto IT incidentu analīzes (ziņotie pārtraukumi palīdzības dienestā).

6.1.3. Efektīva un atbildīga resursu pārvaldība

6.1.3.1. Ārkārtējās situācijas pārvarēšanas zināšanu koplietošana

Atsevišķiem uzņēmumiem un organizācijām vienatnē nepietiek spējas un resursi, lai risinātu ārkārtas situācijas, tādēļ ir nepieciešama to savstarpējā sadarbība. Sadarbību rekomendēts veicināt zināšanu koplietošanas un zināšanu apmaiņas veidā. Uzņēmumu kopums, kas sadarbojas savstarpēji bagātinoties, veido drošu un noturīgu servisu sniegšanas tīklu jeb ekosistēmu.

6.1.3.2. Efektīvas un drošas komunikācijas veicināšana un pārvaldība

Globālās pandēmijas rezultātā būtiski mainījies darba komunikācijas veids, tā piespiedu kārtā kļuva atkarīga no tehnoloģijām. Komunikācijā, kas balstīta uz tehnoloģiju izmantošanu svarīgi ir ne tikai tehnoloģiskie aspekti, bet arī vadības un darbinieku spēja efektīvi attālināti komunicēt. Lielākā daļa cilvēku saziņas ir neverbāla un komunikācija izmantojot tehnoloģiskos līdzekļus nav tik efektīva kā tikšanās dzīvē. Neverbālās komunikācijas signāli parasti netiek pārraidīti caur tehnoloģiju. Šī jaunā digitālā darba vide rada jaunas problēmas un izaicinājumus uzņēmumu vadītājiem. Papildus darbiniekiem ir iespējami psiholoģiski sarežģījumi kā pandēmijas radītā stresa blakusfaktors.

Efektīvas un drošas komunikācijas nodrošināšanai uzņēmumiem rekomendēts:

- Uzņēmumam savlaicīgi izstrādāt vadlīnijas rīcībai piespiedu distancēšanās apstākļos, kas sevī ietvertu risinājumus kā:
 - nodrošināt vai atrunāt interneta pieejamību;
 - nodrošināt vai atrunāt digitālo ierīču pieejamību;
 - nodrošināt darbiniekus ar nepieciešamajām ierīcēm un programmatūrām;
 - nodrošināt darbiniekiem drošu piekļuvi sistēmām un resursiem tiešsaistē;
 - apmācīt darbiniekus par minimālajām drošības prasībām strādājot tiešsaistē;
 - apmācīt vadītājus un darbiniekus darbam tiešsaistē.
- Efektīvas komunikācijas nodrošināšanai izmantot šādus principus:
 - izvēlēties komunikācijas kanālu atkarībā no konteksta;
 - veikt regulāru saziņu ar darbiniekiem individuāli;
 - organizēt regulāras tiešsaistes sapulces;
 - veidot ziņu garumu atkarībā no konteksta;
 - noteikt komunikācijai nepieciešamo laiku;
 - nodrošināt efektīvu kanālu pieejamību ar iespējām dalīties ar failiem, balsi, video un teksta ziņām;

- nodrošināt datu repozitoriju pieejamību, kuros vienlaikus pie viena faila var strādāt vairāki darbinieki;
- nodrošināt vadītājus ar atbalsta funkciju.
- Rekomendācijas komunikācijai uzņēmuma rīkotajās sapulcēs (t.i. video konferencēs) un izmantojot elektronisko saziņu:
 - iedrošināt darbiniekus ikdienā savā starpā komunicēt arī neformāli;
 - izmantot kādus no sociālajiem tīkliem, lai būvētu emocionālo kapitālu;
 - nodrošināt regulāras tikšanās;
 - skaidri definēt sapulču struktūru;
 - iepazīstināt ar elektroniskās sarakstes sūtīšanas pieklājības normām (struktūra, atbilžu sniegšanas laika rāmji un adresāti);
 - vērst uzmanību uz emocionālā stāvokļa ietekmi uz elektronisko saraksti un cita veida saziņu (piemēram, e-pastus nevajadzētu sūtīt esot bēdīgā vai emocionāli uzbudinātā stāvoklī);
 - video konferenci sākt ar sanāksmes vadītāja uzrunu un sanāksmes dalībnieku pārskatīšanu (t.i. apzināšanu kas ir/nav ieradies uz sanāksmi);
 - video konferences laikā tās dalībnieki nedrīkst veikt blakus sarunas (piemēram, pa telefonu);
 - sapulces sākumā norādīt uz formu, kādā sapulces dalībnieki var uzdot jautājumus.
- Drošas komunikācijas nodrošināšanai izmanto šādus principus:
 - ievērot darba devēja vadlīnijās par attālināto darbu noteikto;
 - darba vajadzībām rekomendējams izmantot tikai darba devēja ierīces;
 - darba vajadzībām izmantot tikai drošu interneta pieslēguma veidu;
 - informācijas sistēmām un resursiem pieslēgties izmantojot virtuālo privāto tīklu (*virtual private network - VPN*);
 - darbu uz darbstacijas (t.sk. elektronisko ziņojumu sūtīšanu) veic nodrošinot, ka trešās personas neredz ierīces ekrānā izvadīto un/vai ievadāmo tekstu;
 - izmantot drošās failu sūtīšanas vai kopdarba pie viena faila iespējas;
 - ārpus darba telpām video sanāksmēs piedalīties tikai izmantojot austiņas un mikrofonu;
 - dalībnieki, kas sanāksmē piedalās ar video, nodrošina ka tiem aizmugurē ir neitrāls fons, izmanto rīka fona piedāvātos attēlus vai aizmiglo fonu;
 - atrodoties publiskās vietās atbildes sniegšanai pa telefonu izmantot tikai vispārīgas, nepersoniskas frāzes, kā arī izvērtēt nepieciešamību sarunu turpināt brīdī, kad darbinieks atradīsies nostāk no sabiedrības;
 - gadījumos, kad tiek pārrunāti īpaši nozīmīgi jautājumi, ar video starpniecību pārliecināties, ka saruna notiek ar konkrēto personu;
 - pirms dalīties ar ekrānu, pārliecināties, ka kādā no atvērtajiem logiem nav redzama ierobežotas pieejamības informācija, personas dati u.tml.;
 - video sanāksmes laikā ekrānā dalīties tikai ar tiem dokumentiem, kas nav ierobežotas pieejamības informācija u.tml.;
 - video sanāksmes ierakstīšanu veikt tikai galējas nepieciešamības gadījumā, nodrošināt drošu ieraksta uzglabāšanu un ierobežot piekļuvi tam;
 - veikt darbinieku apmācību par drošiem komunikācijas veidiem un citiem ar informāciju tehnoloģijām saistītiem drošības jautājumiem, periodiski kontrolēt drošības nosacījumu izpildi.

6.1.3.3. Darbinieku motivācijas līmeņa monitorings

Viens no galvenajiem efektīvas komunikācijas mērķiem ir motivēti un apmierināti darbinieki. Darbinieku motivācija un apmierinātība būtiski aspekti attālināta darba apstākļos, jo īpaši laikā, kad līdz šim informāciju un komunikāciju tehnoloģiju izmantošana nav bijis pamatmērķis. Tajā pašā laikā jāatceras un jāņem vērā, ka darbinieku psiholoģiskā labsajūta ir neatņemama darba kvalitātes sastāvdaļa.

Lai apzinātu darbinieku motivācijas līmeni un identificētu nepieciešamos pasākumus tā celšanai, rekomendēts veikt darbinieku motivācijas līmeņa monitoringu. Darbinieku motivācijas līmeņa monitoringam rekomendēts veidot aptaujas un regulāri komunicēt ar darbiniekiem. Viena iespēja kā mērīt motivāciju un apmierinātību ir izmantojot patērētāju lojalitātes rādītāju (*net promoters score - NPS*).

6.1.3.4. Digitālo ekosistēmu izveide resursu optimizācijai

Digitālo pakalpojumu ekosistēmas ir savstarpēji papildinošs organizāciju tīkls, kas nodrošina digitālo pakalpojumu sniegšanu. Uzņēmēji veido pakalpojumu ekosistēmas, kas veido vienotu sadarbības vidi, apvienojot dažādus pakalpojumu sniedzējus un piegādātājus (Subramaniam, Iyer, & Venkatraman, 2019). Uzņēmumi ekosistēmās pērk un pārdod pakalpojumus, integrē biznesa procesus un pakalpojumus un rada jaunu vērtību klientiem. Ekosistēmas nodrošina lietotājoorientētu pieeju, personalizētus pakalpojumus un to izmantošana vairums gadījumos samazina katra individuālā komersanta izmaksas par digitālo pakalpojumu sniegšanu. Ekosistēmu pamatā ir vienota informācijas telpa, kas rodas savietojot lielu apjomu organizāciju datus no dažādiem avotus. Šāda telpa paredzēta kā vide un vienota sadarbības valoda dažādām platformām un tehnoloģijām (Mozokhin & Shvedenko, 2019).

Biznesa servisu nodrošināšanai normālā situācijā ekosistēmas var tikt veidotas kombinētu pakalpojumu piedāvāšanai pasažieriem, piemēram, pārvadājums kopā ar negadījumu vai veselības apdrošināšanu, kas radītu lielāku uzticību pakalpojumu sniedzējiem un arī pavērtu jaunu pakalpojumu iespējas. Tomēr jāņem vērā, ka ekosistēmu darbināšana rada papildus drošības riskus - organizāciju sadarbības rezultātā veidojas arī vienotas risku un apdraudējumu ekosistēmas. Salīdzinot ar "tradicionālo" pakalpojumu sniegšanu vienas organizācijas ietvaros, riski digitālajās ekosistēmās ir daudz augstāki. "Tradicionālajos" modeļos katra organizācija pārvalda savus riskus. Digitālajās ekosistēmās risku pārvaldība ir kopīgs process, organizācija nav spējīga pilnībā kontrolēt drošības aspektus, atbildība par informācijas drošības nodrošināšanu ir jāuzņemas katram sadarbības partnerim. Risku mazināšanai organizācijām pirms sadarbības uzsākšanas ieteicams veikt padziļinātu sadarbības partneru izpēti un trešo pušu risku novērtējumu. Uzsākot sadarbību iesaistītajām pusēm, jāveido kopīgi ekosistēmu risku novērtējumi un jāievieš atbilstoši drošības pasākumi (datu apmaiņas aizsardzība, piekļuves kontroles u.c.). Tāpat kopīgi plānojama ekosistēmu darbības nepārtrauktība un atjaunošana.

6.1.3.5. Digitālā ētika kā uzņēmuma politikas sastāvdaļa

Digitālā ētika ir atbildīga tehnoloģiju izmantošana. Līdz ar tehnoloģiju attīstību, nozīmīgāki paliek tehnoloģiju atbildīgas un pārskatāmas izmantošanas aspekti (Yasser & Adel, 2019). Digitālās ētikas principus rekomendēts integrēt tehnoloģiju izmantošanas politikā, katram darbiniekam ir jāuzņemas atbildība par tehnoloģiju un datu izmantošanu attālinātajā darbā, t.sk., izmantojot tīkla pakalpojumus. Uzņēmumiem ieteicams digitālās ētikas aspektus atrunāt iekšējos normatīvajos dokumentos, kā arī izglītēt organizāciju darbiniekus (Kongnso, 2015), piemēram, veidojot informācijas kampaņas, apmācības vai īstenojot "digitālo vēstnešu" programmas (Matzner, 2017). Digitālās ētikas nodrošināšanai

izmantojamas šādas tehnoloģijas: SIEM sistēmas lietotāju un tehnoloģiju (piemēram, mākslīgais intelekts) veikto darbību analīzei, datu pārvaldības un piekļuves vadības sistēmas datu izmantošanas pārskatāmības nodrošināšanai.

6.1.3.6. Digitālo prasmju un digitālo spēju stiprināšana

Digitālo prasmju un spēju trūkums ir viens no būtiskākajiem IKT izmantošanas kavējošajiem faktoriem, līdz ar to uzņēmumiem būtu nepārtraukti mērķtiecīgi jāveicina darbinieku digitālo prasmju un spēju celšana.

Digitālo prasmju celšana tiek attiecināta uz dažādām mērķauditorijām, no kurām īpaši tiek izcelti mazie un vidējie uzņēmumi (MVU) un publiskās pārvaldes iestādes. Eiropas Komisija rekomendē nodrošināt, lai pašreizējais un turpmākais darbaspēks spētu viegli apgūt augsta līmeņa digitālās prasmes, jo īpaši augstas veiktspējas datošanas, mākslīgā intelekta un kiberdrošības jomā, piedāvājot studentiem, absolventiem un pašreizējiem darba ņēmējiem iespējas apgūt un pilnveidot šīs prasmes neatkarīgi no viņu atrašanās vietas (Eiropas Komisija, Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, 2018). Padziļinātu digitālo prasmju celšanai uzņēmumiem rekomendēts regulāri nodrošināt digitālo prasmju apmācības dažādās formās, t.sk., nodrošināt digitālo mācīšanās vidi un kursus (piemēram, nodrošināt atvērto izglītības resursu abonentus, ieviest E-apmācību sistēmas).

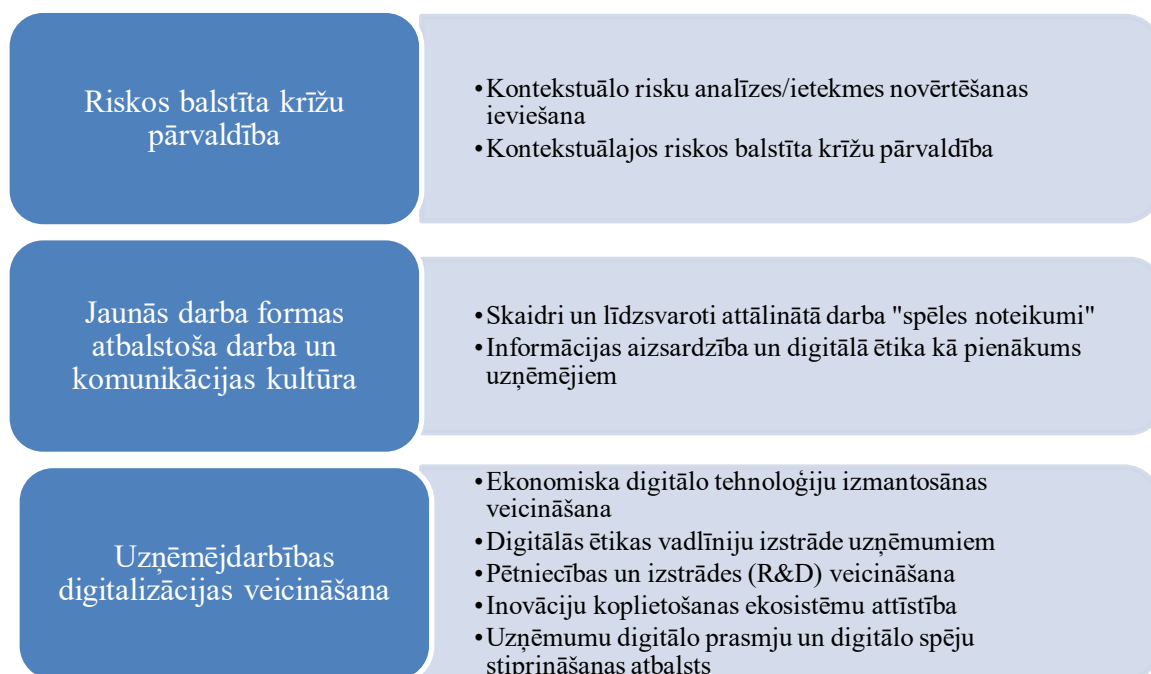
Digitālo spēju paaugstināšana tiek attiecināta uz spējām izmantot dažādas IKT tehnoloģijas, īpaši uzsvērot spējas augstas veiktspējas datošanas, mākslīgā intelekta un kiberdrošības jomā (Eiropas Komisija, Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, 2018). Digitālo spēju paaugstināšanas tendences katrā no programmas "Digitālā Eiropa" jomām ir aprakstītas specifiskās tehnoloģijas aprakstā (augstas veiktspējas datošana, kiberdrošība u.c.). Kopīgās spēju paaugstināšanas tendences ir:

1. Dalība digitālo inovāciju centros, kompetences centros un izcilības centros;
2. Dalība zināšanu apmaiņu tīklos;
3. Starptautiskā sadarbība, publiskā un privātā partnerība.
4. Inovāciju infrastruktūras un atbalsta mehānismu pieejamības nodrošināšana, resursu un datu koprade un koplietošana.

6.2. Priekšlikumi valsts atbalstam un intervencei

Priekšlikumi valsts atbalstam un intervencei aptver trīs galvenos virzienus (Ilustrācija 18):

4. Risku analīzē balstīta krīžu pārvaldība – priekšlikumi kontekstuālo risku analīzei un riskos balstītai krīžu pārvaldībai, plānojot uzņēmējdarbības atbalstu un valsts intravenci;
5. Jaunās darba formas atbalstoša darba un komunikācijas kultūra – priekšlikumi noteikumu un vadlīniju izveidei valsts līmenī;
6. Uzņēmumu digitalizācijas veicināšana – priekšlikumi valstiski veicamajiem pasākumiem uzņēmumu digitalizācijas veicināšanai.



Ilustrācija 18 Priekšlikumi valsts atbalstam un intravencei

6.1.1. Risku analīzē balstīta krīžu pārvaldība

6.1.1.1. Kontekstuālo risku analīzes/ietekmes izvērtēšanas ieviešana

Valsts līmenī ir jāveic kompleksa kontekstuālo risku analīze, lai pieņemot lēmumus tie samērīgi atbilstu sabiedrības interesēm. Šobrīd Attīstības plānošanas likuma 4. pants nosaka „Attīstības plānošanas dokumentā **izvirza mērķus un sasniedzamos rezultātus attiecīgā politikas jomā vai teritorijā, apraksta noskaidrotās problēmas un paredz to risinājumus, izvērtē šo risinājumu iespējamo ietekmi**, kā arī plāno turpmāko politikas īstenošanai un rezultātu novērtēšanai nepieciešamo rīcību”. Tātad šobrīd, saskaņā ar likumu, ietekmes novērtējums (izņemot ietekmi uz vidi un budžetu) tiek veikts tikai katras konkrētās politikas jomā vai tikai konkrētās teritorijas ietvaros.

Attīstības plānošanas likumā tiek paredzēts, ka Ministru kabinets nosaka attīstības plānošanas dokumentu un tiesību aktu iespējamās ietekmes izvērtēšanas (izņemot stratēģisko ietekmes uz vidi novērtējumu) kārtību, ciktāl likumā nav noteikts citādi.

Šobrīd Ministru kabineta 02.12.2014. noteikumi nr.737 „Attīstības plānošanas dokumentu izstrādes un ietekmes izvērtēšanas noteikumi” neprecizē kāds ietekmes novērtējums ir jāveic. Līdz ar to, ņemot vērā Attīstības plānošanas likumā noteikto ietvaru, tiek vērtēta plānošanas dokumenta (tajā paredzēto pasākumu) vai normatīvā akta ietekme uz nozari, teritoriju, valsts vai pašvaldības budžetu un noteiktos gadījumos – uz vidi.

Izmantojot risku analīzes pieeju mūsdienu apstākļos plānošanas dokumentiem un normatīvajiem aktiem būtu nepieciešams izvērtēt:

- **populācijas un sabiedrības apsvērumus (ietekme uz demogrāfiju, iedzīvotāju dabiskā un mehāniskā kustība, iespēja nodrošināt cilvēka cienīgus dzīves apstākļus ar likumīgi pieejamiem līdzekļiem, drošību un pašlāvību uz valsts institūcijām, publisko pakalpojumu pieejamību, kultūru un nācijas identitāti u.c..)**

- **uzņēmējdarbības apsvērumus (infrastrukturā pieejamību, darba spēka pieejamību, tirgus pieejamību, nodokļu un nodevu sistēmas samērīgumu un prognozējamību u.c.);**

Ievērojot, ka krīzes seku likvidēšanai un vispārējai situācijas uzlabošanai vienlaikus dažādās nozarēs tiek veikti atšķirīgi pasākumi, kuriem, iespējams, ir kopīgi (vai radniecīgi) mērķi (piemēram, izmaiņas atsevišķos nodokļu maksāšanas režīmos ar mērķi papildināt valsts budžetu un sniegt sociālo nodrošinājumu noteiktu profesiju pārstāvjiem) ir jāveic kompleks ietekmju un risku novērtējums.

Risku analīzei un ietekmju izvērtēšanai ir ieteicams veidot vienotu zināšanu pārvaldības sistēmu, kura spēj nodrošināt situācijas modelēšanu un datu analīzi, kā tas tiek piedāvāts ARTSS projektā. Šādas sistēmas izveide ir kompleks pasākums, kur informācijas uzkrāšanā ir nepieciešama visu valsts pārvaldes struktūru, kā arī sociālo partneru iesaistīšanās.

6.1.1.2. Kontekstuālos riskos balstīta krīžu pārvaldība

Epidemioloģiskās krīzes laikā lēmumus par situācijas kontroles pasākumiem pieņem krīzes vadības padome.

Saskaņā ar Nacionālās drošības likuma (turpmāk NDL) 23². pantu, krīzes vadības padomi vada Ministru prezidents un tās sastāvā ietilpst aizsardzības, ārlietu, ekonomikas, finanšu, iekšlietu, tieslietu, veselības, satiksmes, kā arī vides un reģionālās attīstības ministri.

Atbilstoši NDL 23³. pantam, krīzes vadības padome koordinē valsts apdraudējuma pārvarēšanas operatīvo vadību un valsts pārvaldes institūciju valsts apdraudējuma novēršanas plānu izstrādi, kā arī koordinē politisko lēmumu vienotu un savlaicīgu izpildi valsts pārvaldes institūcijās.

Savukārt ministrijas prognozē to kompetencē esošo nozaru apdraudējumus un plāno apdraudējumu novēršanu, pārvarēšanu un iespējamo seku likvidēšanu. Nozaru apdraudējumu novēršanas, pārvarēšanas un iespējamo seku likvidēšanas plānus ministrijas iesniedz apstiprināšanai attiecīgajiem Ministru kabineta locekļiem. Plānu projektus pirms apstiprināšanas ministrijas iesniedz izvērtēšanai Krīzes vadības padomē. Apstiprinātos plānus ministrijas iesniedz Krīzes vadības padomē izmantošanai padomes darbā.

Apdraudējumu analīze ir viena no risku vadības sastāvdaļām. Šobrīd pamatā tiek pievērsta uzmanība epidemioloģiskajiem apdraudējumiem, mazāk domājot par kontekstuālajiem riskiem un ar to saistītajiem apdraudējumiem. Pamatā ir četras apdraudējumu (ievainojamības) grupas: fiziskie, sociālie ekonomiskie un vides apdraudējumi (P.Coppola, 2015). Apdraudējumu (un ievainojamības) elementi ir savstarpēji saistīti. Ekonomiskie apdraudējumi var novest pie sociālas ievainojamības, kas savukārt var radīt vides un fiziskos apdraudējumus (P.Coppola, 2015).

Šobrīd Nacionālās drošības padomes lēmumos dominē epidemioloģiskās drošības jautājumi bez pietiekama citu ietekmju (apdraudējuma, ievainojamības) izvērtējuma.

Latvijas tirdzniecības un rūpniecības kameras prezidents 2020. gada 24. novembrī portālam "Delfi" pauž šādu viedokli (Rostovskis, 2020): „Šī gada pavasarī, krīzei sākoties, Latvijas Tirdzniecības un rūpniecības kamera aicināja valdību izstrādāt krīzes pārvarēšanas stratēģiju, un, lai pēc iespējas vispusīgāk vadītu krīzi, grupā pie šī plāna izveides strādātu gan valdības pārstāvji, gan plašs profesionāļu loks no dažādām jomām. Pēc ilgas pārliecināšanas darba grupa tika izveidota Ekonomikas ministrijas paspārnē, taču krīzes vadības plāns tapa diemžēl tikai attiecībā uz tautsaimniecības daļu, un pat tas netiek pilnvērtīgi realizēts.”

Tas norāda ka pamatā tiek domāts tikai par epidemioloģiskajiem pasākumiem un pienācīga uzmanība netiek pievērsta ekonomiskajai krīzei, kas savukārt var izraisīt finanšu un sociālo krīzi.

Pēc definīcijas, krīze ir notikums, kas, ja tam ļauj saasināties, var pārtraukt organizācijas ikdienas darbu un apdraud tās reputāciju, kā arī grauj pamatbūtību (Siliņa, 2018).

Lai radītu pamatu sabiedrības noturībai sociālajā un ekonomiskajā jomā epidemioloģiskās krīzes apstākļos ir jāievieš pilnvērtīgi krīzes pārvaldības mehānismi atbilstoši krīžu pārvaldības labākajai praksei izvērtējot ne tikai epidemioloģiskos, bet arī kontekstuālos riskus un ietekmes.

Digitālie risinājumi, zināšanu uzkrāšana, kā arī modelēšanas instrumenti var sniegt būtisku atbalstu krīzes pārvaldībā, palīdzot analizēt daudzveidīgas pieejas uzņēmējdarbības atbalstam.

6.1.2. Jaunās darba formas atbalstoša darba un komunikācijas kultūra

6.1.2.1. Skaidri un līdzsvaroti attālinātā darba “spēles noteikumi”

Ārkārtējās situācijas izsludināšana prasīja operatīvu attālinātā darba ieviešanu tajās nozarēs un uzņēmumu funkcijās, kur tas bija iespējams no darba specifikas viedokļa.

Grozījumi darba aizsardzības likumā tika apstiprināti stājās spēkā 2020. gada 1. jūlijā un būtiskākie jautājumi attiecībā uz darba apstākļiem un darba vidi tiek regulēti.

Grozījumi darba likumā šī pētījuma sagatavošanas brīdī atrodas Saeimā, 3.lasījumā paredz, ka, gadījumā, ja darbinieks un darba devējs vienojas par darba veikšanu attālināti, darbinieka izdevumus, kas saistīti ar attālināto darba veikšanu, sedz darba devējs, ja darbinieks un darba devējs nav vienojušies citādi.

No uzņēmēju viedokļa ir svarīgi, lai izdevumi, kas uzņēmējam rodas sedzot darbinieka izdevumus, kas saistīti ar attālinātā darba veikšanu, netiktu aplikti ar darbaspēka nodokļiem, tādējādi palielinot uzņēmēja izmaksas.

Gan darbiniekiem, gan uzņēmējiem pilnvērtīgi ir jāizmanto dažādi nodarbinātības veidi, tajā skaitā digitalizācijas ietekmē radītie – attālinātais darbs, platformu ekonomika, automatizācija, nepilna laika nodarbinātība u.c..

Nepieciešams veikt pasākumus jauno nodarbinātības veidu pareizai, taisnīgai un efektīvai izmantošanai, lai tiktu izveidoti tādi noteikumi, kas būtu skaidri un godīgi pret abām pusēm – darbinieku un darba devēju. (NAP norāda, ka šobrīd tas netiek pienācīgi izmantots (Pārresoru koordinācijas centrs, Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam., 2020)).

6.1.2.2. Informācijas aizsardzība un digitālā ētika kā pienākums uzņēmējiem

Aizvien plašāka digitālo tehnoloģiju izmantošana ikdienā veicinās aizvien lielāka datu apjoma radīšanu un uzkrāšanu, kas savukārt radīs visdažādākos riskus, ja šo datu uzglabāšanu un atkalizmantošanu nebūs iespējams pilnvērtīgi kontrolēt. Šajos apstākļos būtisku nozīmi iegūst digitālās ētikas pamatprincipu ievērošana ikviena uzņēmuma darbā un informācijas aizsardzības jautājumi atkalizmantošanas kontekstā.

Ja fizisko personu datu aizsardzības jautājumi Latvijā ir samērā labi reglamentēti, tad informācijas drošības un digitālās ētikas principu ieviešanai ir pārrobežu raksturs un to ievērošanas kontrole ir sarežģīta un pat cilvēka spēkiem neiespējama.

Digitālās ekonomikas lielākā vērtība ir dati. Konkurences apstākļos uzņēmumi vāc, glabā, analizē, izmanto un izplata datus tik plaši kā nekad iepriekš. No vienas puses tas dod iespēju radīt vairāk personalizētu produktu un pakalpojumu, kas rezultējas kā uzņēmumu ieņēmumi. No otras puses tas rada šaubas par datu izmantošanas ētiskumi, precizitāti, caurskatāmību un pienācīgu privātuma aizsardzību (Deloitte, 2020).

Īpašas prasības tas izvirza arī tehnoloģijām, kas tiek izmantotas datu uzglabāšanai un pārraidīšanai. Piemēram, Igaunijas parlaments ir pieņēmis Elektronisko sakaru likumu, kura mērķis ir garantēt, lai telekomunikāciju tīklos nākotnē tiek izmantotas drošas tehnoloģijas no drošiem partneriem. Likuma preambulā bija norādīts, ka 5G tīklu veidošanā nedrīkst piedalīties nedemokrātiskas valstis, kurām ir vara pār to jurisdikcijā esošajiem uzņēmumiem, kā arī uzsvērts, ka lēmumiem informācijas tehnoloģiju jomā jābūt tādiem, lai uz tiem varētu paļauties arī Igaunijas sabiedrotie Ziemeļatlantijas līguma organizācijā (Ukenābele, 2020).

Ieviešot digitalizācijas risinājumus uzņēmumiem ir nepieciešamas informācijas drošības un digitālās ētikas politikas, kas nosaka vismaz informācijas vākšanas, uzglabāšanas un atkalizmantošanas principus ievērojot ētikas normas un privātuma aizsardzību, kā arī prasības izmantotajām tehnoloģijām no informācijas aizsardzības viedokļa. Šādu politiku nepieciešamību rekomendēts noteikt par obligātu valsts līmenī.

6.1.3. Uzņēmējdarbības digitalizācijas veicināšana

6.1.3.1. Motivējošie faktori digitālo tehnoloģiju izmantošanas veicināšanai

G→B un B→G komunikācijā uzņēmēju ieinteresētību izmantot digitālos risinājumus var palielināt, ja valsts un pašvaldību pakalpojumi tiešsaistē izmaksātu mazāk nekā izmantojot klasiskos pakalpojumu piegādes kanālus – klātienē apmeklējumu un pastu. Klientu pārvirzīšanu uz digitālajiem pakalpojumu sniegšanas/saņemšanas kanāliem iespējams efektīvi novirzīt izmantojot valsts un pašvaldību nodevas, t.i. nosakot zemākas nodevas par pakalpojumu saņemšanu, ja komunikācija notiek digitāli. No uzņēmēju viedokļa ekonomiskais izdevīgums tiek uzskatīts par prioritāru un tas ir motivējošāk nekā finansējums apmācībām vai tamlīdzīgi pasākumi.

Likums „Par nodokļiem un nodevām” nosaka, ka valsts nodeva ir obligāts maksājums valsts budžetā vai šajā likumā noteiktajos gadījumos pašvaldības budžetā par valsts vai pašvaldības institūcijas veicamo darbību, kas izriet no šīs institūcijas funkcijām. Valsts nodevas mērķis ir personu darbību regulēšana (kontrolēšana, veicināšana, ierobežošana). Valsts nodevas apmērs nav tiešā veidā saistīts ar institūcijas veiktās darbības izmaksu segšanu.

Latvijas Valsts kontrole regulāri kopš 2009. gada ir sniegusi Finanšu ministrijai ieteikumus valsts nodevu administrēšanas sistēmu sakārtošanā. Piemēram, Valsts kontrole ir norādījusi, ka uz 2016. gada beigām Latvijā noteikti 114 valsts nodevu veidi, to apmērus un maksāšanas kārtību nosaka deviņi likumi un vairāk nekā 100 Ministru kabineta noteikumi. Nodevas tiek ieskaitītas 71 valsts budžeta kontā. Revīzijas ziņojuma sagatavošanas brīdī valsts nodevu administrēšanas procesā bija iesaistītas apmēram 50 institūcijas, 42 tiesas, 23 zemesgrāmatu nodaļas, 47 diplomātiskās un konsulārās pārstāvniecības, 101 zvērināts tiesu izpildītājs, kā arī 109 zvērināti notāri (Valsts kontrole, 2017).

Izstrādājot regulējumu valsts un pašvaldību nodevu administrēšanai, ir iespējams paredzēt noteikumus, kas ļauj nodevas apmēru koriģēt atkarībā no komunikācijas kanāla. Ja nodevas apmēra samazinājums ļaus uzņēmējiem samazināt savu preču un pakalpojumu pašizmaksu, tie būs daudz aktīvāki digitālo kanālu izmantošanā.

6.1.3.2. Pētniecības un izstrādes (R&D) veicināšana

Rekomendēts veicināt pētniecības un izstrādes (R&D) apjomu digitālu tehnoloģiju kopradei un koplietošanai, stiprinot sadarbību starp pētniecības institūcijām un uzņēmējiem. Valsts līmenī rekomendēts turpināt realizēt līdzīgas programmas kā esošā kompetenču centru programma RIS3 jomās, kā arī praktisko pētījumu programmas. Programmās būtiski nodrošināt atbalsta mehānismus īpaši mazo un vidējo uzņēmumu (MVU) segmentam, lai stiprinātu to digitālās spējas. Tāpat nozīmīgi ir Digitālo inovāciju hubi, kas palīdzētu uzņēmējiem transformēties digitālajā vidē.

6.1.3.3. Inovāciju koplietošanas ekosistēmas attīstība

Inovāciju koplietošanas infrastruktūra ir atklāto datu un pirmkoda izmantošana un zināšanu apmaiņa. Inovāciju koplietošanas infrastruktūra tiek realizēta gan atvērta koda risinājumu veidā, ko uzņēmumiem iespējams pielietot inovāciju izveidei, gan arī koplietošanas risinājumu un atvērto datu veidā. Koplietojamus risinājumus primāri veido publiskās pārvaldes iestādes un uzņēmējdarbībā tie izmantojami komunikācijai un datu apmaiņai G2B un B2G segmentos. Tipiski koplietošanas risinājumi ir datu apmaiņas platformas (piemēram, uzņēmumu un valsts datu apmaiņai) un elektroniskās identitātes risinājumi. Inovāciju infrastruktūra tiek koplietota arī B2B segmentā, piemēram, nozares uzņēmumi mēdz veidot kopējas datu ekosistēmas.

Valsts pārvalde ir labi pieņēmusi klasiskos un aprobētos IKT risinājumus un to ieviešanas pieejas, taču neskatoties uz to, ka IKT nozare attīstās ar vien straujāk un pastāvīgi kļūst pieejami arvien jauni tehnoloģiskie risinājumi, darbības modeļi un metodes, kas ļauj vēl efektīvāk īstenot valsts pārvaldes digitālo attīstību, valsts pārvalde kūtri ietver šos risinājumus sava IKT nodrošinājuma izvēļu arsenālā (VARAM, Digitālās transformācijas pamatnostādnes 2021-2027. gadam. Projekts., 2021).

Arī risku pieejas ieviešana krīžu pārvaldībā pieprasa iespēju veikt situāciju modelēšanu, lai izstrādātu sabiedrības interesēm atbilstošākos rīcības scenārijus. ARTSS pieeja, izstrādātie modeļi un metode var radīt pamatu digitālo un institucionālo inovāciju aprobācijai publiskās pārvaldes ekosistēmā.

Valsts līmenī rekomendēts attīstīt uzņēmumiem paredzētos e-pakalpojumus (īpaši pašvaldību), paplašināt un atvērt uzņēmējiem valsts koplietošanas risinājumus (datu atļaujas, integrācijas platforma u.c.). Rekomendēts uzlabot uzņēmēju e-pakalpojumu un uzņēmēju izmantojamo Valsts informācijas sistēmu lietojamību (piemēram, Būvniecības informācijas sistēma). Tāpat valstiski rekomendēts izvērtēt uzņēmumu digitalizācijas simulācijai un biznesa nepātrauktības plānošanai izmantojamu digitālo dvīņu izveidi. Papildus tehnoloģiskajiem risinājumiem, būtiski nodrošināt arī konsultācijas (piemēram, juridiskās un IT konsultācijas par elektronisko grāmatvedības dokumentu apriti, rēķini, pavadzīmes u.c.).

Valsts līmenī rekomendēts turpināt datu atvēršanu un to izmantošanas uzņēmējdarbībā veicināšanu. Būtiski atvērt jēgpilnus datus, kas tiešām ir nepieciešami, piem., nederīgo dokumentu reģistrs, daļa PMLP datu.

6.1.3.4. Uzņēmumu digitālo prasmju un digitālo spēju stiprināšana

Rekomendēts veicināt uzņēmumu digitālā brieduma līmeņa paaugstināšanos, stiprinot uzņēmumu digitālās prasmes un spējas.

Digitālo prasmju un spēju paaugstināšanai rekomendēts turpināt īstenot apmācību programmas (piemēram, macibaspieaugusajiem.lv, uzņēmumu mācību grupas). Būtiski apmācībās iekļaut informācijas drošības, digitālās ētikas un personas datu aizsardzības jomas. Mācībās iekļaujamas arī programmā “Digitālā Eiropa” definētās stratēģiskās digitālās spējas (Eiropas Komisija, Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, 2018) – augstas veikspējas datošana, mākslīgais intelekts un kibersdrošība.

Papildus mācību programmu realizācijai, uzņēmumu digitālo spēju stiprināšanas veicināšanai rekomendēts veidot un uzturēt metodikas par kopējiem digitalizācijas aspektiem, piemēram, elektronisku dokumentu pieņemšanu (elektroniskās pavadzīmes, rēķini) un nozaru specifiskajiem digitalizācijas risinājumiem (piem., BIM būvniecībā). Zināšanas par nozaru specifiskajiem risinājumiem, cita starpā, konceptualizējamas nozaru digitalizācijas paraugmodeļu veidā.

Literatūra

1. Aguiar, T., Boga Gomes, S., Rupino da Cunha, P., & Mira da Silva, M. (2019). Digital Transformation Capability Maturity Model Framework. *2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC)* (lpp. 51-57). Paris: IEEE.
2. Aguiar, A., Roland, W., & Twardowski, T. (2018). Perspectives on bioeconomy. *New Biotechnology*, 181-184.
3. Albukhitan, S. (2020). Developing Digital Transformation Strategy for Manufacturing. *Procedia Computer Science*, 664–671.
4. CERT. (2020. gada Aprīlis). *Kiberlaikapstākļi (aprīlis)*. Ielādēts no <https://cert.lv/lv/2020/05/kiberlaikapstakli-aprilis>
5. CERT. (2020). *Par telefonkonferenču rīku drošību*. Ielādēts no [cert.lv/https://cert.lv/lv/2020/04/par-telekonferencu-riku-drosibu](https://cert.lv/lv/2020/04/par-telekonferencu-riku-drosibu).
6. COMMISSION OF THE EUROPEAN COMMUNITIES. (2008). *Report on the implementation of the European social partners Framework Agreement on Telework*.
7. Culot, G., Orzes, G., Sartor, M., & Nassimbeni, G. (2020). The future of manufacturing: A Delphi-based scenario analysis on Industry 4.0. *Technol Forecast Soc Change*.
8. Dārziņa, L. (2020). <https://lvportals.lv/>. Ielādēts no Jaunas normas darba aizsardzībā – attālinātajam darbam un pašnodarbinātajiem: <https://lvportals.lv/skaidrojumi/317440-jaunas-normas-darba-aizsardziba-attalinatajam-darbam-un-pasnodarbinatajiem-2020>
9. Deloitte. (2020). *Owning digital responsibility and ethics. Future of risk in the digital era*. Ielādēts no [www2.deloitte.com:https://www2.deloitte.com/us/en/pages/advisory/articles/digital-ethics.html](https://www2.deloitte.com/us/en/pages/advisory/articles/digital-ethics.html).html
10. Derksen, C., & Weber, C. (2017). *Smart Energy Research. At the Crossroads of Engineering, Economics, and Computer Science*. Essen: Springer.
11. Eiropas Komisija. (2018). *HPC - BEST USE EXAMPLES*. Ielādēts no High performance computing best use cases: <https://ec.europa.eu/digital-single-market/en/news/high-performance-computing-best-use-examples>
12. Eiropas Komisija. (2018). *Koordinētais mākslīgā intelekta plāns*. Ielādēts no Eiropas Komisijas [tīmekļa vietne:https://ec.europa.eu/transparency/regdoc/rep/1/2018/LV/COM-2018-795-F1-LV-MAIN-PART-1.PDF](https://ec.europa.eu/transparency/regdoc/rep/1/2018/LV/COM-2018-795-F1-LV-MAIN-PART-1.PDF)
13. Eiropas Komisija. (2018). *Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu*. Ielādēts no Eur-LEX tīmekļa vietne: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=COM:2018:434:FIN>
14. Eiropas Komisija. (2019). *2019. gada Eiropas pusgads - novērtējums par progresu strukturālo reformu īstenošanā, makroekonomikas nelīdzsvarotības novēršanā un koriģēšanā, un saskaņā ar Regulu (ES) Nr. 1176/2011 veikto padziļināto pārskatu rezultāti*. Ielādēts no https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-latvia_lv.pdf

15. Eiropas Komisija. (2020). *Digitālās ekonomikas un sabiedrības indekss (DESI) 2020. gadā Latvija*.
16. Eurofound. (2020). <https://www.eurofound.europa.eu>. Ielādēts no COVID-19 EU PolicyWatch: <https://www.eurofound.europa.eu/lv/data/covid-19-eu-policywatch>
17. Eurofound. (2020). *Living, working and COVID-19, COVID-19 series*. Luxembourg: Publications Office of the European Union.
18. Eurofound and the International Labour Office. (2017). Ielādēts no Working anytime, anywhere: The effects on the world of work, Publications Office of the European Union, Luxembourg, and the International Labour Office, Geneva.
19. European Commission. (2017). *New interoperability framework*. European Commission.
20. European Commission. (2017). *New Interoperability Framework*. European Commission.
21. European Commission. (2020). *Joinup EC Europa*. Ielādēts no European interoperability reference architecture (EIRA): <https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-3-views-viewpoints-and-architecture-building-blocks>
22. Eurostat. (2020). <https://ec.europa.eu/eurostat/>. Ielādēts no How usual is it to work from home?: <https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/DDN-20200424-1>
23. Fana et al. (2020). *Fana, M., Milasi, S., Napierala, J., Fernandez Macias, E. anTelework, work organisation and job quality during the COVID-19 crisis: a qualitative study, European Commission, 2020, JRC122591*. Luxembourg: European Commission.
24. Fisseler, D., Kemény, Z., & Reiners, R. (2016). Monitoring and Control Framework for Business Processes in Ubiquitous Environments. *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress* (lpp. 863-868). IEEE.
25. Gigova, T., Valeva, K., & Nikolova-Alexieva, V. (2019). Digital transformation-opportunity for industrial growth. *In International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019* (lpp. 1-4). Sandanski: IEEE.
26. Goncarovs, P. (2019). Active Learning SVM Classification Algorithm for Complaints Management Process Automatization. *2019 60th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)* (lpp. 1-3). Riga: IEEE.
27. Yasser, A., & Adel, A. (2019). Digital Ethics and Privacy: A study about digital ethics issues, implications, and how to solve them.
28. JANSONS, A., & STIVRIŅA, D. (2020). <https://lvportals.lv/>. Ielādēts no Šodienas realitāte – attālinātais darbs. Kam piemērotāks un kā organizējams?: <https://lvportals.lv/viedokli/314858-sodienas-realitate-attalinatais-darbs-kam-piemerotaks-un-ka-organizejams-2020>
29. Kantar. (2020). *Kantar*. Ielādēts no Kas strādājošajiem Latvijā nepatīk/ pietrūkst un kas – patīk, domājot par ikdienas darbu ārkārtējās situācijas laikā?:

- <https://www.kantar.lv/tnsab60/kas-stradajosajiem-latvija-nepatik-pietrukst-un-kas-patik-domajot-par-ikdienas-darbu-arkartejas-situacijas-laika/>
30. Kantar. (2020). *Koronavīrusa radītā situācija joprojām ietekmē 31% Latvijas iedzīvotāju ikdienu un turpina ietekmēt sabiedrības uzvedību*. Ielādēts no www.kantar.lv/ : <https://www.kantar.lv/tnsab61/koronavirusa-radita-situacija-joprojam-ietekme-31-latvijas-iedzivotaju-ikdienu-un-turpina-ietekmet-sabiedribas-uzvedibu/>
 31. Kongnso, F. (2015). *Best practices to minimize data security breaches for increased business performance*. Ielādēts no scholarworks.waldenu.edu: scholarworks.waldenu.edu
 32. Kotamarthi, K., Wang, X., Grossmann, G., Sheng, Q., & Indrakanti, S. (2015). A Framework Towards Model Driven Business Process Compliance and Monitoring. *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop* (lpp. 24-32). Adelaide: IEEE.
 33. Ladekar, S. (2014). *Best Practices for Information Security Breach Management*. Ielādēts no www.researchgate.net: https://www.researchgate.net/publication/264084730_Best_Practices_for_Information_Security_Breach_Management
 34. Laibach, N., Börner, J., & Bröring, S. (2019). Exploring the future of the bioeconomy: An expert-based scoping study examining key enabling technology fields with potential to foster the transition toward a bio-based economy. *Technology in Society*, 58.
 35. Latvijas Republikas Finanšu ministrija. (2020). *Finanšu ministrijas mājaslapa*. Ielādēts no FM: Ekonomikas izaugsme Latvijā trešajā ceturksnī strauji atjaunojusies, perspektīvas atkal apdraud COVID: https://www.fm.gov.lv/lv/sadalas/tautsaimniecibas_analize/tautsaimniecibas_analize/i-ekszemes_kopprodukts/62924-fm-ekonomikas-izaugsme-latvija-tresaja-ceturksni-strauji-atjaunojusies-perspektivas-atkal-apdraud-covid-19
 36. Latvijas Republikas Ministru kabinets. (2020). *Likumprojekta "Grozījumi Darba aizsardzības likumā" sākotnējās ietekmes novērtējuma ziņojums (anotācija)*. Rīga.
 37. Latvijas Televīzija. (2020). <https://www.lsm.lv/>. Ielādēts no Aptauja: Covid-19 krīzes laikā 22% pārgājuši uz attālināto darbu: <https://www.lsm.lv/raksts/zinas/latvija/aptauja-covid-19-krizes-laika-22-pargajusi-uz-attalinato-darbu.a353939/>
 38. Li, B., Dong, M., Shang, J., & Zhao, P. (2018). Design and Implementation of Business Processes Efficiency Analysis System. *2018 IEEE 4th International Conference on Computer and Communications (ICCC)* (lpp. 2175-2179). IEEE.
 39. LIKTA. (2020). www.gudralatvija.lv/. Ielādēts no <https://www.gudralatvija.lv/>
 40. Maldaner, N., Tomkins-Lane, C., Desai, A., Zygorakis, C., Weyerbrock, A., Gautschi, O., & Stienen, M. (2020). Digital transformation in spine research and outcome assessment. *Spine Journal*.
 41. Markvarte, N. (2020). Informācijas tehnoloģijas risinājumu spektrs industrijā 4.0. Rīga.
 42. Matzner, T. (2017). Data science education as contribution to media ethics. *In Paderborn Symposium on Data Science Education at School Level 2017*, (lpp. 28).

43. Michel A., C., & Michielin, O. (2020). Digitalization is Fueling a Revolution in Precision Oncology. *Systems Medicine*, 342-346.
44. Mogorite, I., & Didenko, K. (2012). Pretkrīzes vadīšana uzņēmuma krīzes dzīves ciklā. *Economics and Business. Economics and Business 2012/22 p.135.*, 135.
45. Mozokhin, A., & Shvedenko, V. (2019). Digitization development directions of national and foreign energy systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 657–672.
46. Mullen et al. (2020). *Operational Toolkit for Businesses Considering Reopening or Expanding Operations in COVID-19*. The Johns Hopkins Center for Health Security.
47. Noy, I., Doan, N., & Benno, F. (2020). <https://voxeu.org/article/economic-risk-covid-19-not-where-covid-19>.
48. OECD. (2018). *GOING DIGITAL IN A MULTILATERAL WORLD*. Ielādēts no www.oecd.org: <https://www.oecd.org/going-digital/C-MIN-2018-6-EN.pdf>
49. OECD. (2020). *A systemic resilience approach to dealing with Covid-19 and future shocks*. Ielādēts no www.oecd.org: <http://www.oecd.org/coronavirus/policy-responses/a-systemic-resilience-approach-to-dealing-with-covid-19-and-future-shocks-36a5bdfb/>
50. OECD. (2020). *Going Digital in Latvia*.
51. OECD. (2020). *Productivity gains from teleworking in the post COVID-19 era : How can public policies make it happen?* Ielādēts no www.oecd.org : <https://www.oecd.org/coronavirus/policy-responses/productivity-gains-from-teleworking-in-the-post-covid-19-era-a5d52e99/#section-d1e973>
52. P.Coppola, D. (2015). *Introduction to International Disaster Management*. Woburn, United States: Elsevier Science & Technology.
53. Pārresoru koordinācijas centrs. (2013). *Nacionālās attīstības plāns 2014.-2020*. Ielādēts no <https://www.pkc.gov.lv/>: <https://www.pkc.gov.lv/lv/attistibas-planosana-latvija/nacionalais-attistibas-plans>
54. Pārresoru koordinācijas centrs. (2020). *Latvijas Nacionālais attīstības plāns 2021. – 2027. gadam*. Rīga: Pārresoru koordinācijas centrs;
55. Pelēce, D. (2020). *Makroekonomika.lv*. Ielādēts no Nākotnes tūrisms - viesniču burziņš vai distancēšanās Latvijas plāvās?: <https://www.makroekonomika.lv/nakotnes-turisms-viesnicu-burzins-vai-distancesanas-latvijas-plavas>
56. Plyatsuk, L., Chernysh, Y., Ablieieva, I., Bataltsev, Y., Vaskin, R., Roy, I., & Roubík, H. (2020). Modelling and development of technological processes for low rank coal bio-utilization on the example of brown coal. *Fuel*.
57. Pumpiņš. (2020). Jaunās darba organizācijas formas. Rīga.
58. Rīgas Tehniskā universitāte. (2014). *RĪCĪBAS PLĀNS ATTĀLINĀTĀ DARBA VEICINĀŠANAI UN ATTĀLINĀTĀ DARBA CENTRU VEIDOŠANAI LATVIJĀ*. Rīga: Rīgas Tehniskā universitāte.
59. Rostovskis, A. (2020). *Aigars Rostovskis: Krīzes laikā neprofesionāli lēmumi nav pieļaujami*. Ielādēts no www.delfi.lv/: <https://www.delfi.lv/news/versijas/aigars-rostovskis-krizes-laika-neprofesionali-lemumi-nav-pielaujami.d?id=52687457>

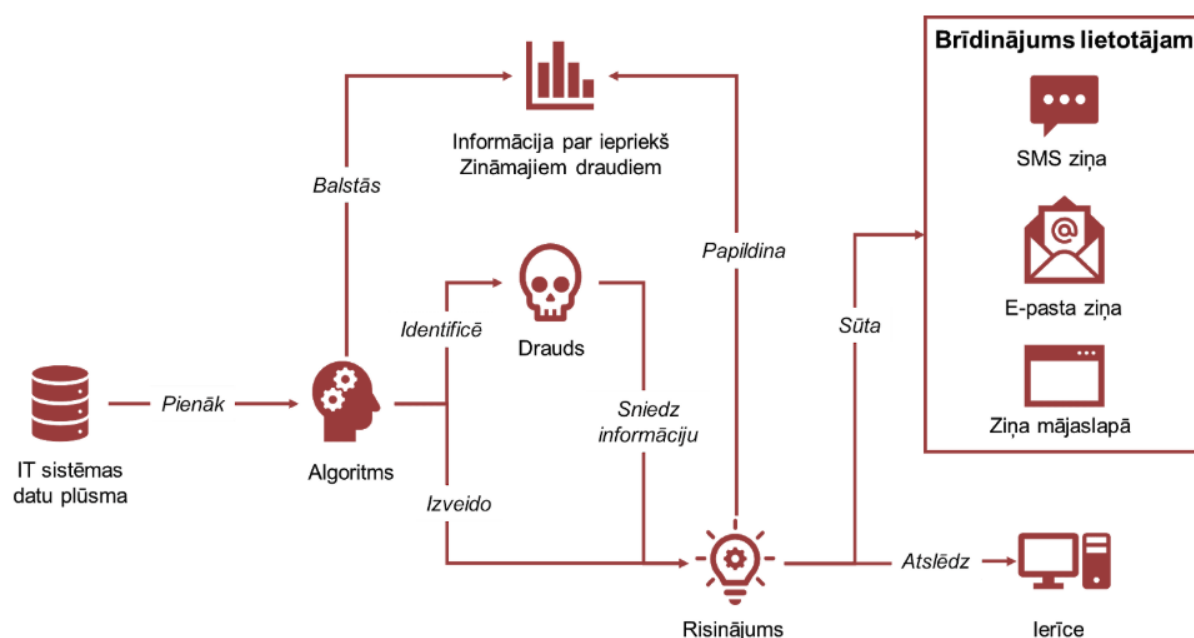
60. Salkin, C., Oner, M., Ustundag, A., & Cevikcan, E. (2018). A Conceptual Framework for Industry 4.0. *Springer Series in Advanced Manufacturing*, 3-23.
61. Schrettenbrunnner, M. (2020). Artificial-Intelligence-Driven Management. *IEEE Engineering Management Review*, 15-19.
62. Siliņa, R. (2018). *Krīžu komunikācija*. Mācību matereāls Valsts kancelejas administrētā projektā "Atbalsts strukturālo reformu ieviešanai valsts pārvaldē" 3.3.aktivitātes „Valsts pārvaldes analītisko spēju uzlabošana” ietvaros.
63. Subramaniam, M., Iyer, B., & Venkatraman, V. (2019). Competing in digital ecosystems. *Business Horizons*, 83-94.
64. Tele2. (2020). <https://www.tele2.lv/>. Ielādēts no #paliecējās pētījums: strādāt attālināti arī turpmāk vēlas 32% Latvijas iedzīvotāji: https://www.tele2.lv/tele2/tele2-jaunumi/jaunums/paliecējās-petijums-stradat-attalinati-/?utm_source=twitter&utm_medium=social&utm_campaign=SocialComm
65. Tilde. (2020). <https://nra.lv/>. Ielādēts no Aptauja: kas visvairāk traucē strādāt attālināti?: <https://nra.lv/latvija/313766-aptauja-kas-visvairak-trauce-stradat-attalinati.htm>
66. Ukenābele, I. (2020). *Cīņā par 5G tīkla ieviešanu Eiropa mēģina balansēt starp savām interesēm un brīvu konkurenci*. Ielādēts no <https://www.lsm.lv/>: <https://www.lsm.lv/raksts/zinas/ekonomika/cina-par-5g-tikla-ieviesanu-eiropa-megina-balanset-starp-savam-interesem-un-brivu-konkurenci.a382928/>
67. Valsts kontrole. (2017). *Valsts kontrole norāda uz nepilnībām valsts nodevu administrēšanas sistēmā*. Ielādēts no www.delfi.lv: https://www.delfi.lv/business/budzets_un_nodokli/valsts-kontrole-norada-uz-nepilnibam-valsts-nodevu-administresanas-sistema.d?id=49314111
68. Vandvik, P., & Brandt, L. (2020). Future of Evidence Ecosystem Series: Evidence ecosystems and learning health systems: why bother? *Journal of Clinical Epidemiology*, 166-170.
69. VARAM. (2013). *Koncepcija par publisko pakalpojumu sistēmas pilnveidi*. Ielādēts no www.varam.gov.lv: Koncepcija par publisko pakalpojumu sistēmas pilnveidi. Izgūts https://www.varam.gov.lv/lv/publisko-pakalpojumu-sistemas-pilnveide-1/koncepcija_publ_pak_sist_pilnv.pdf.
70. VARAM. (2019). *Informatīvais ziņojums par mākslīgā intelekta attīstību*. Rīga.
71. VARAM. (2021). *Digitālās transformācijas pamatnostādnes 2021-2027. gadam. Projekts*. Ielādēts no www.varam.gov.lv: https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf
72. Xiao, L. (2020). Optimal Allocation Model of Enterprise Human Resources Based on Particle Swarm Optimization. *2020 International Conference on Computer Information and Big Data Applications (CIBDA)* (lpp. 249-253). Guiyang: IEEE.

1.pielikums “Droša un noturīga servisa piemērs”

ARTSS metodes projektā tiek izmantota vairāku lietošanas gadījumu analīzei. Viens no lietošanas gadījumiem ir droši pamatservisi, kas analizē servisu datortīkla drošības pārvaldībai.

Droši pamatservisi

Pamatservisi ir tādi, kas nodrošina citu digitālo pakalpojumu darbību un drošu tīklošanu. Tā kā pandēmijas seku dēļ liela daļa ekonomikas un mācību notiek tiešsaistē, ļaunprātīgas darbības datortīklā būtu jānosaka pēc iespējas ātrāk.



Ilustrācija 19 Drošu pamatservisu nodrošināšanas konceptuālais modelis

Spējas modelis

Šajā piemērā ir apskatīta droša universitātes tīkla pārvaldības spējas modelis, kuru ir iespējams pielāgot citas sistēmas/organizācijas vajadzībām.

Organizācijas datortīkla darbībai krīzes apstākļos ir nepieciešama spēja droši pārvaldīt tās datortīklu. Šo spēju raksturo vairāki mērķi, kuru izpilde tiek novērtēta ar KPI palīdzību:

1. Nodrošināt drošu IT vidi – šis mērķis ir sadalīts 3 zemāk redzamajos mērķos,
2. Novērst drošības incidentus – ātra incidentu atrisināšana. Novērtē ar:
 - Incidentu atrisinājuma laiku,
 - Incidentu skaitu.
3. Minimizēt CERT brīdinājumus. Novērtē ar:
 - Brīdinājumu skaitu mēnesī,
4. Nodrošināt augstu savienojuma kvalitāti – savienojuma ātrums, nav noildzes un zudis savienojums. Novērtē ar:

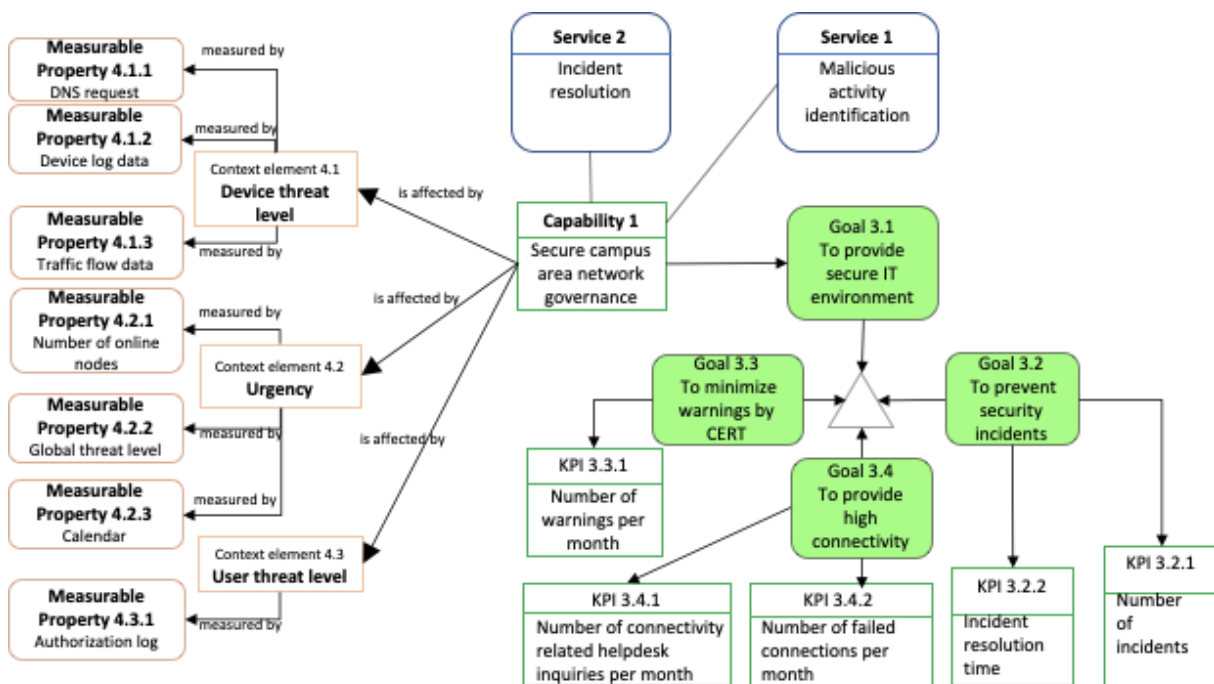
- Neveiksmīgu savienojumu skaitu mēnesī.

Spējas nodrošināšanai ir nepieciešami datortīkla pārvaldības servisi. Pamatfunkcionalitāti nodrošina datortīkla pārvaldības programmatūra. Tā tomēr nespēj nodrošināt visas vajadzības ārkārtas situācijā, tādēļ tiek izmantoti papildus servisi drošības un noturības nodrošināšanai:

1. Ļaundabīgas aktivitātes identificēšanas serviss – izmanto dažādas tehnikas inficēto tīmekļa mezglu noteikšanai,
2. Incidentu atrisināšanas serviss – piedāvā dažādas lietotāja informēšanas aktivitātes incidenta risināšanai.

Spējas sasniegšanu ietekmē konteksta elementi, kuru ietekmes līmeni (zems, vidējs, augsts, nezināms) ir iespējams izmērīt ar mērāmo datu vienību). Spējas modeļa konteksta elementi ir iedalīti 2 konteksta elementu kopās: Iekārtas draudu līmenis (1.,2.,3. konteksta elements), Atslēgt iekārtu (2., 3. konteksta elements). Spējas modeļa konteksta elementos ietilpst:

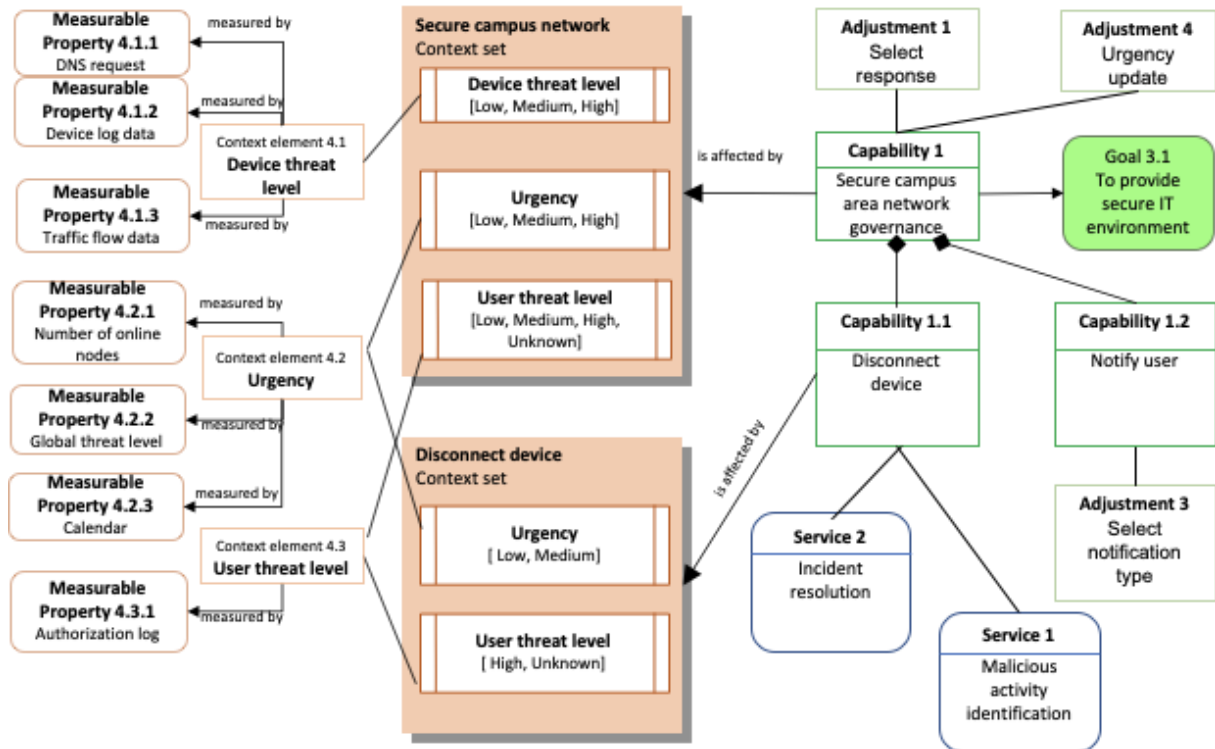
1. Iekārtas draudu līmenis – norāda, vai iekārta ir potenciāli inficēta. Novērtē ar:
 - DNS pieprasījumu skaitu – aizdomīgu vai ļaunprātīgu DNS izsaukumu skaits,
 - Iekārtas log dati – informācija, kad iekārta ir bijusi pieslēgta tīklam.
2. Steidzamība – apraksta vajadzību pēc iespējas ātrāk atrisināt incidentu. Novērtē ar:
 - Tiešsaistes iekārtu skaits,
 - Globālais draudu līmenis – norāda, cik daudz draudu ir šobrīd,
 - Kalendārs.
3. Lietotāja draudu līmenis – norāda, vai lietotājs varētu būt ļaunprātīgs. Novērtē ar:
 - Autorizācijas log dati – informācija, kad lietotājs bija pieslēgts tīklam un kāda ir bijusi tā uzvedība.



Ilustrācija 20 Drošas tīkla pārvaldības spējas modelis: mērķi un konteksts

Papildus spējas atbilstoši mūsu sistēmas gadījumam piedāvā 2 iespējamās sistēmas reakcijas:

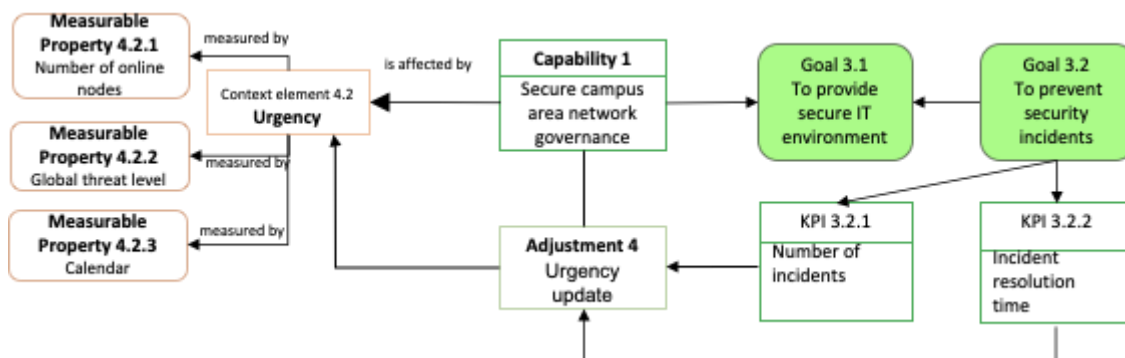
1. Atslēgt iekārtu – kas tiek pielietots, ja tiek novērtēts, ka lietotājs ir ļaunprātīgs, vai ja lietotājs nereaģē uz informatīvajiem paziņojumiem,
2. Paziņot lietotājam – izmantojot pielāgojumu Izvēlēties paziņojuma tipu, informē lietotāju.



Ilustrācija 21 Drošas tīkla pārvaldības spējas modelis: pielāgojumi

Spējas modelis ir papildināts ar pielāgojumiem, nodrošinot dinamisku modeļa pielāgošanos sistēmas apstākļiem un tā atbilstību sistēmai:

1. Izvēlēties atbildes veidu – norāda, kura no papildus spējām (Paziņot lietotājam vai atslēgt ierīci) tiks izmantota, ņemot vērā kontekstu un KPI,
2. Izvēlēties paziņojuma tipu - norāda, kādu tipu no 3 ziņojumu veidiem (ziņa mājaslapā, e-pasta ziņa vai SMS ziņa) izmanto lietotāja informēšanai,
3. Steidzamības atjauninājums – dinamiski pielāgo incidentu steidzamību, ņemot vērā globālo incidentu skaitu un incidenta atrisinājuma laiku.



Ilustrācija 22 Drošas tīkla pārvaldības spējas modelis: mērķi un konteksts

2.pielikums “Rekomendācijas komandu kopdarbības rīkiem”

Komunikācijas rīki

Attālinātā darbā nozīmīga ir pieejama un efektīva komunikācija, līdz ar to ir nepieciešams nodrošināt piemērotus komunikācijas un sadarbības rīkus. Komunikāciju ir svarīgi fiksēt, lai tā būtu pieejama visiem (arī tiem, kas reālā sarunā nav klāt), kā arī lai būtu pieejama pilna komunikācijas vēsture un ērta meklēšana tajā. Komunikācijas rīki uzlabo komunikācijas ātrumu un efektivitāti.

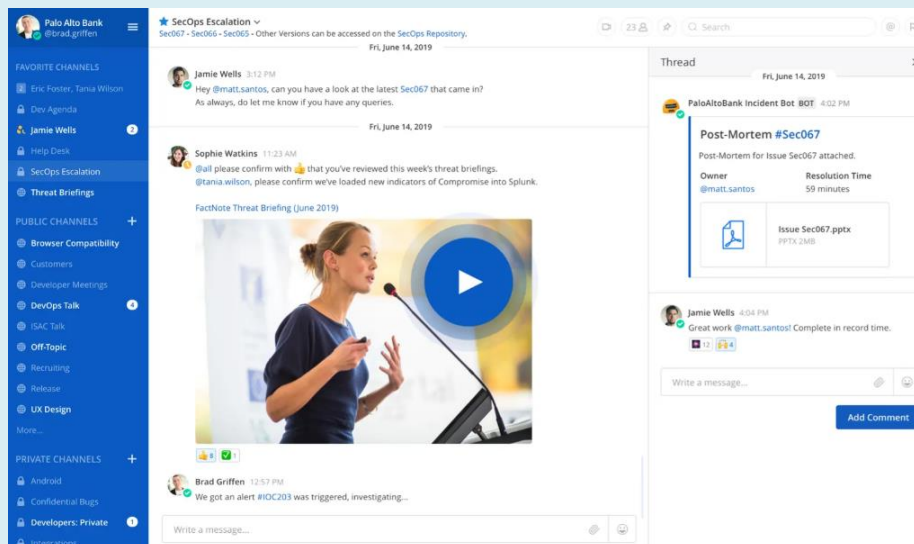
Bieži vien mazi un vidēji uzņēmumi aprobežojas ar e-pastu, Skype, Whatsapp vai saziņu pa tālruni, tomēr šādu rīku izmantošana nenodrošina efektīvu komunikāciju.

Mūsdienās eksistē modernas ziņapmaiņas platformas, kas nodrošina dažāda veida komunikāciju un sadarbību.


Komunikācijas rīku piemēri – brīvprogrammatūras rīki



- Fleksibla atvērta koda ziņapmaiņas platforma, kas nodrošina drošu komandas sadarbību / komunikāciju
- Pieejama gan darbvirsmas (*desktop*), gan mobilā lietotne
- Iespēja veidot piekļuvi tikai uzņēmuma darbiniekiem
- Priekšrocības:
 - Iespējams organizēt sarunas komandās un kanālos
 - Balss, video un ekrāna kopīgošana
 - Failu, attēlu un saišu koplietošana
 - Ērta un pilnīga meklēšana pilnā sarunu vēsturē
 - Emocijzīmes, teksta formatējums
 - Daudzvalodu atbalsts
 - Atslēgas vārdu pieminēšanas paziņojumu iestatījumi
 - Pielāgojamas darbvirsmas, e-pasta un mobilie paziņojumi u.c.



Komunikācijas rīku piemēri – komerciālie produkti



- Ziņapmaiņas platforma, kas nodrošina drošu komandas sadarbību / komunikāciju
- Pieejama gan darbvirsma (*desktop*), gan mobilā lietotne
- Iespēja veidot piekļuvi tikai uzņēmuma darbiniekiem
- Priekšrocības:
 - Ļoti plašas integrācijas iespējas ar citiem uzņēmumā izmantotajiem rīkiem, piemēram, JIRA
 - Iespējams organizēt sarunas komandās un kanālos
 - Ērta un pilnīga meklēšana pilnā sarunu vēsturē ar papildus filtriem
 - Ir pieejams virtuālais asistents – slackbots
 - Balss un video zvanu iespējas
 - Ekrāna koplietošanas iespējas u.c.

Kopsadarbības rīki


Kopsadarbības rīki ļauj projekta komandām efektīvi kopsadarboties ar mērķi nodrošināt labāku projekta sniegumu.

Kopsadarbības rīki nodrošina dažādu funkcionalitāti:

- Ziņapmaiņu
- Video konferences zvanus
- Reāla laika kopsadarbību
- Uzdevumu pārvaldību
- Failu pārsūtīšanu
- Projekta monitoringu

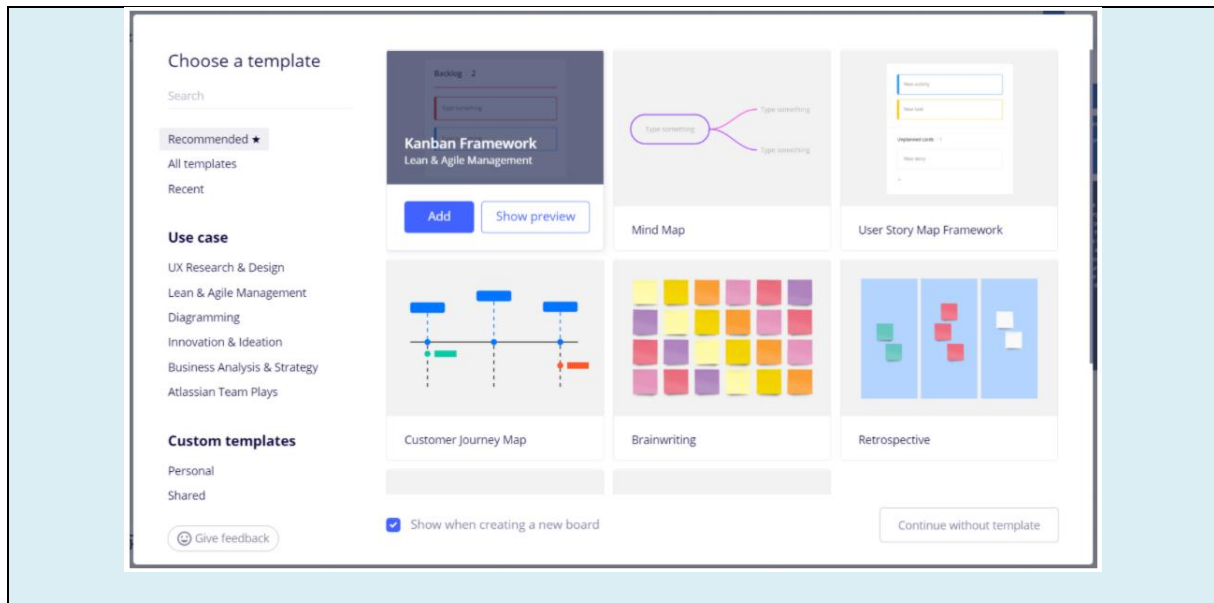
Ja komanda strādā attālināti, ir vērts izmantot digitālus kopsadarbības rīkus, kas palīdz nodrošināt efektīvu komandas komunikāciju. Digitālās kopsadarbības tāfeles ļauj projekta komandām kopsadarboties, risinot problēmas, ģenerējot idejas un radot risinājumus

Kopsadarbības rīku piemēri – rīki ar pieejamu brīvprogrammatūras versiju



MIRO digitālā kopdarbības tāfele

- Komandu kopdarbības rīks
- Pieejama mobilā lietotne
- Iespēja veidot piekļuvi tikai uzņēmuma darbiniekiem
- Priekšrocības:
 - Ļoti plašs veidņu piedāvājums (piemēram, ideju ģenerēšanas veidnes, problēmu risināšanas veidnes u.c.)
 - Iespējams apmainīties ar ziņām ar komandas dalībniekiem
 - Reālā laikā iespējams redzēt citu komandas dalībnieku veiktās darbības
 - Pielāgojamas darbvirsma, e-pasta un mobilie paziņojumi u.c.



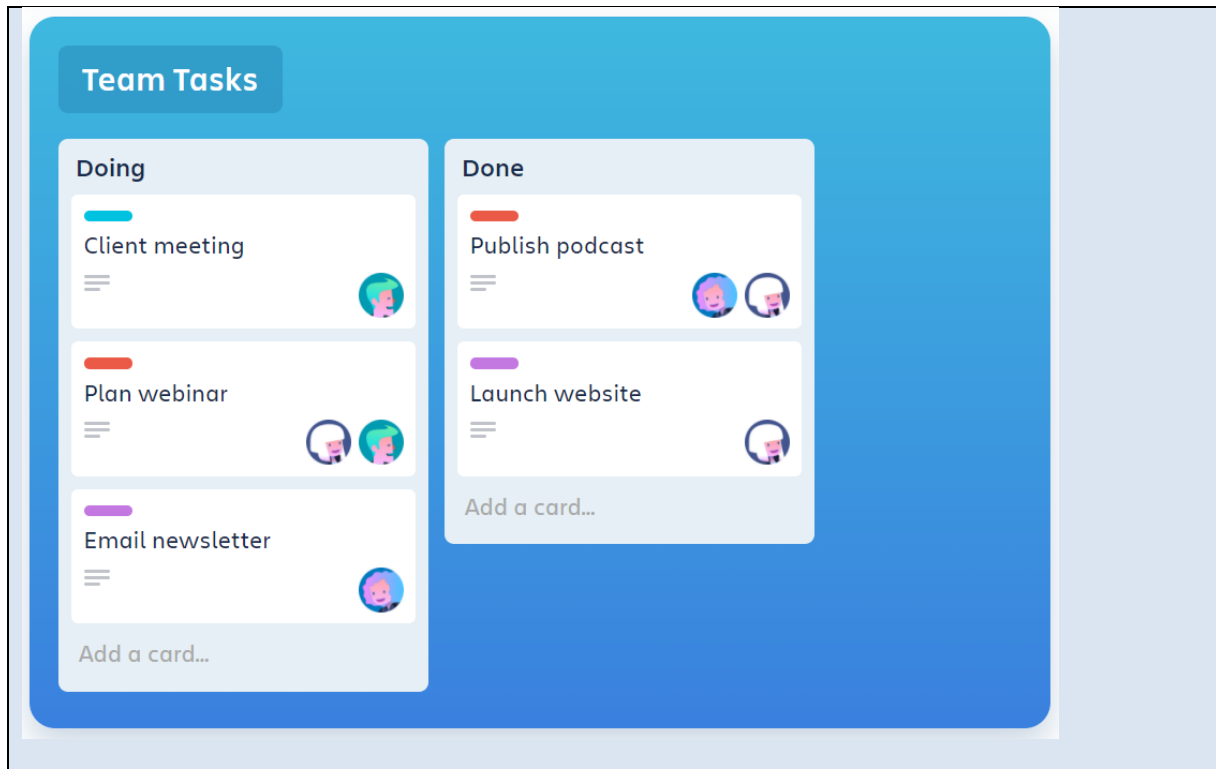
Darbu plānošanas rīki

Darbu plānošanai un izpildes pārskatam rekomendēts izmantot darbu plānošanas rīkus, piemēram, vizualizējot komandu darbus Kanban dēļos. Tipiski šāda pieeja tiek izmantota IT nozares uzņēmumos un projektos, bet to iespējams pārņemt arī citās nozarēs.

Darbu plānošanas rīku piemēri – rīki ar pieejamu brīvprogrammatūras versiju



- Darbu plānošanas un pārvaldības dēļis
- Priekšrocības:
 - Vienkārša darbu vizualizācija (darāmie darbi, progresā esošie darbi, pabeigtie darbi)
 - Iespējama sasaiste ar kalendāriem
 - Plašas integrācijas iespējas ar citiem rīkiem (piemēram, informācijas koprades rīkiem)

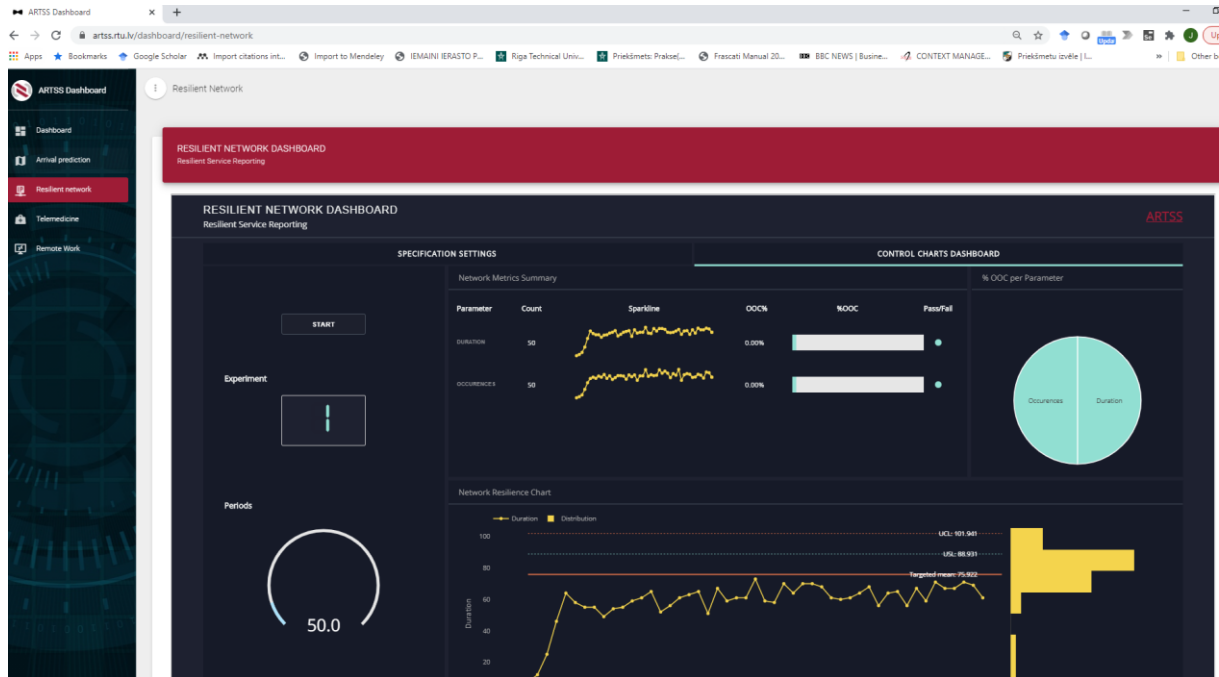


3.pielikums “Šablona piemērs”

Nosaukums	Videokonferenču rīku kvalificēšana
Atslēgas vārds	<ul style="list-style-type: none"> • Attālinātais darbs
Problēma	Noteikt, kurus videokonferences tīklus drīkst izmantot saziņai
Mērķis	<ul style="list-style-type: none"> • Nodrošināt pieslēgšanos saziņas kanālam • Nepieļaut sesijas traucēšanu • Nodrošināt personas datu aizsardzības prasības • Nodrošināt videokonferences efektīvu norisi
Lietderīguma rādītāji (KPI)	-
Konteksts	<ul style="list-style-type: none"> • Servisa lietotāju vērtējums • Servisa sertifikācija • Servisa ievainojamības
Risinājums	<ul style="list-style-type: none"> • Izvēlas videokonferenču rīku ar augstu vērtējumu un atbilstošu sertifikācijas prasībām • Ievainojamību novērtēšanai izmanto CVE reģistru • Lietotāju vērtējuma novērtēšanai izmanto Google Play un Apple App Store
Risinājuma elements	-
Ievadparametrs	<ul style="list-style-type: none"> • Sertifikācijas prasības
Ievadparametru vērtības	<ul style="list-style-type: none"> • GDPRP • HIPAA

4.pielikums “Digitālā dvīņa piemērs”

Drošu pamatservisu digitālā dvīņa vizuāls attēlojums sniegts Ilustrācija 23. Attēlā redzams studentu pilsētiņas datortīkla digitālais dvīnis, kurā tiek monitorēts un analizēts incidentu pārvaldības process. Digitālais dvīnis saņem datortīkla reāllaika datus, identificē drošības notikumus un potenciālos incidentus un novērtē to kritiskuma un steidzamības līmeņus.



Ilustrācija 23 Digitālā dvīņa piemērs

5.pielikums “Tehnoloģiju izmantošanas rekomendācijas”

Tehnoloģijas izmantošana uzņēmējdarbībā		Uzņēmuma brieduma līmenis			
Lietošanas gadījums	Tehnoloģiju pielietojums	1.līmenis	2.līmenis	3.līmenis	4.līmenis
Drošs attālināts darbs	IT risku analīze	Excel izklājlapas	Datu vizualizācijas rīki	Datu noliktavas Datu vizualizācijas rīki Incidentu pārvaldības sistēmas Monitoringa sistēmas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GRC sistēmas Monitoringa sistēmas SIEM sistēmas Mākslīgais intelekts
	Darbu izpildes efektivitātes novērtējums	Excel izklājlapas	Datu vizualizācijas rīki Darbu vizualizācijas dēļi	Datu noliktavas Datu vizualizācijas rīki Darbplūsmu pārvaldības sistēmas Personālpārvaldības sistēmas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki Uzņēmumu resursu pārvaldības sistēmas Darbplūsmu pārvaldības sistēmas Mākslīgais intelekts
	Darbinieku motivācijas monitorings	Aptauju rīki	Datu vizualizācijas rīki Aptauju rīki	Datu noliktavas Datu vizualizācijas rīki Personālpārvaldības sistēmas Aptauju rīki	Mākslīgā intelekta risinājumi Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki Uzņēmumu resursu pārvaldības sistēmas Aptauju rīki Mākslīgais intelekts
	Uzņēmuma komunikācijas efektivitātes novērtējums	Aptauju rīki	Datu vizualizācijas rīki Aptauju rīki Komunikācijas rīki	Datu noliktavas Datu vizualizācijas rīki Komunikācijas rīki Informācijas vietnes Aptauju rīki RPA risinājumi	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki Informācijas vietnes Komunikācijas rīki Aptauju rīki Mākslīgais intelekts
	Procesu darbības	Aptauju rīki	Datu vizualizācijas rīki	Datu noliktavas Datu vizualizācijas rīki	Līdzekļu pārvaldības

Tehnoloģijas izmantošana uzņēmējdarbībā		Uzņēmuma brieduma līmenis			
Lietošanas gadījums	Tehnoloģiju pielietojums	1.līmenis	2.līmenis	3.līmenis	4.līmenis
	monitorings		rīki Aptauju rīki Biznesa procesu pārvaldība (BPM) sistēmas	rīki Biznesa procesu pārvaldība (BPM) sistēmas Aptauju rīki	sistēmas Biznesa procesu pārvaldība (BPM) sistēmas Mākslīgā intelekta risinājumi Uzņēmumu arhitektūras pārvaldības sistēmas Aptauju rīki Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki
Droši pamatservisi	Drošības incidentu analīze	Excel izklājlapas Monitoringa sistēmas	Datu vizualizācijas rīki Incidentu pārvaldības sistēmas Monitoringa sistēmas	Datu noliktavas Datu vizualizācijas rīki Incidentu pārvaldības sistēmas Monitoringa sistēmas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GRC sistēmas Incidentu pārvaldības sistēmas Monitoringa sistēmas SIEM sistēmas 5G tehnoloģijas
	Tīkla noturības monitorings	Excel izklājlapas Monitoringa sistēmas	Datu vizualizācijas rīki Incidentu pārvaldības sistēmas Monitoringa sistēmas	Datu noliktavas Datu vizualizācijas rīki Palīdzības dienesta sistēmas Monitoringa sistēmas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki Palīdzības dienesta sistēmas Incidentu pārvaldības sistēmas Monitoringa sistēmas SIEM sistēmas
Droši biznesa servisi	Maršrutu optimizācija	Maršrutēšanas rīki	Datu vizualizācijas rīki GNSS tehnoloģijas Maršrutēšanas rīki	Datu noliktavas Datu vizualizācijas rīki GNSS tehnoloģijas Maršrutēšanas rīki Transporta vadības sistēmas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki Resursu

Tehnoloģijas izmantošana uzņēmējdarbībā		Uzņēmuma brieduma līmenis			
Lietošanas gadījums	Tehnoloģiju pielietojums	1.līmenis	2.līmenis	3.līmenis	4.līmenis
					optimizācijas sistēmas GNSS tehnoloģijas Ģeotelpiskās informācijas vizualizācijas rīki Transporta vadības sistēmas 5G tehnoloģijas
	Transporta pienākšanas laika prognozēšana	-	Datu vizualizācijas rīki GNSS tehnoloģijas	Datu noliktavas Datu vizualizācijas rīki GNSS tehnoloģijas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GNSS tehnoloģijas Ģeotelpiskās informācijas vizualizācijas rīki 5G tehnoloģijas
	Pasažieru plūsmas monitorings	-	Datu vizualizācijas rīki GNSS tehnoloģijas	Datu noliktavas Datu vizualizācijas rīki GNSS tehnoloģijas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GNSS tehnoloģijas Mākslīgais intelekts 5G tehnoloģijas HCP tehnoloģijas
	Brauciena pārvaldība	-	Datu vizualizācijas rīki GNSS tehnoloģijas	Datu noliktavas Datu vizualizācijas rīki GNSS tehnoloģijas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GNSS tehnoloģijas Transporta vadības sistēmas Ģeotelpiskās informācijas vizualizācijas rīki Mākslīgais intelekts 5G tehnoloģijas HCP tehnoloģijas
	Viedā satiksmes vadība	-	Datu vizualizācijas rīki GNSS tehnoloģijas	Datu noliktavas Datu vizualizācijas rīki GNSS tehnoloģijas 5G tehnoloģijas	Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki GNSS tehnoloģijas

Tehnoloģijas izmantošana uzņēmējdarbībā		Uzņēmuma brieduma līmenis			
Lietošanas gadījums	Tehnoloģiju pielietojums	1.līmenis	2.līmenis	3.līmenis	4.līmenis
					Transporta vadības sistēmas Ģeotelpiskās informācijas vizualizācijas rīki Mākslīgais intelekts 5G tehnoloģijas HCP tehnoloģijas
	Biznesa nepārtrauktības plānošana	Excel izklājlapas	Datu vizualizācijas rīki Aptauju rīki Biznesa procesu pārvaldība (BPM) sistēmas	Datu noliktavas Datu vizualizācijas rīki Biznesa procesu pārvaldība (BPM) sistēmas Aptauju rīki	Biznesa procesu pārvaldība (BPM) sistēmas Mākslīgā intelekta risinājumi Uzņēmumu arhitektūras pārvaldības sistēmas Aptauju rīki Digitālā dvīņa tehnoloģijas Hibrīdi datu analītikas risinājumi – datu noliktavas, datu ezeri, datu straumēšanas rīki, datu vizualizācijas rīki