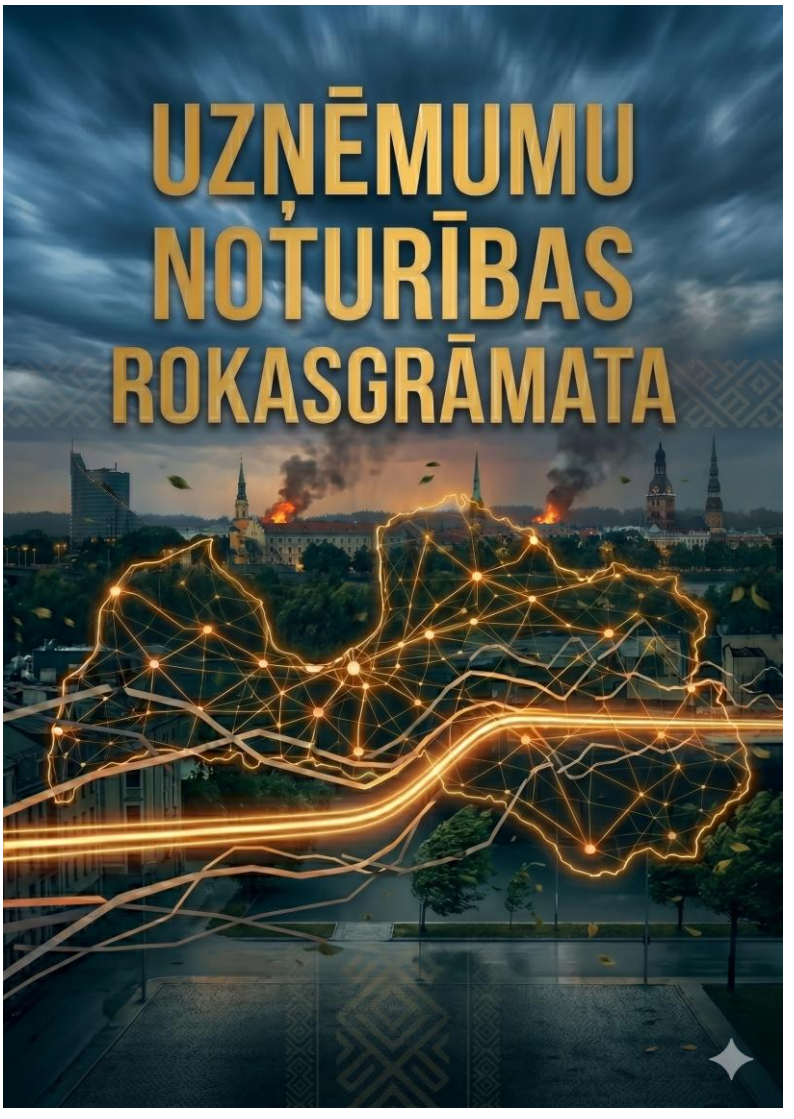
UZŅĒMUMU NOTURĪBAS ROKASGRĀMATA



LATVIAN TRANSATLANTIC ORGANISATION

LATVIJAS REPUBLIKAS
AIZSARDZĪBAS MINISTRIJA

PRIEKŠVĀRDS

Mūsdienās privātais sektors ir kļuvis par daļu no nacionālās drošības sistēmas. Daudzi pakalpojumi ir kritiski svarīgi valsts un visas sabiedrības funkcionēšanai, tādēļ šādu kritisko pakalpojumu nepārtrauktība ir nacionālās drošības jautājums. Vienlaikus šie kritisko pakalpojumu sniedzēji paši mēdz būt atkarīgi no daudziem ārpakalpojumu sniedzējiem un apakšuzņēmējiem, tādēļ jo vairāk uzņēmumu kļūs noturīgāki, jo lielāka varbūtība, ka sabiedrības funkcionēšanai kritiskās funkcijas tiks tiešām nodrošinātas arī apdraudējuma situācijā.

Ukrainas pieredze pierāda, ka tie komersanti, kas spēj pielāgoties krīzei (karš, pandēmija), turpina gūt peļņu. Tādēļ komersantu darbības

nepārtrauktība un gatavība vissliktākajam scenārijam var palīdzēt izdzīvot jebkādu krīzi.

Latvijā uzņēmumu noturības un darbības nepārtrauktības jautājumus nevar skatīt atrauti no visaptverošas valsts aizsardzības, tādēļ rokasgrāmata sadalīta divās daļās:

- Rokasgrāmatas pirmā daļa apskata uzņēmumu noturības jautājumus – primāri, kā sagatavot darbības nepārtrauktības plānu;

- Otrā daļa apskata uzņēmumu rīcību militārā apdraudējuma gadījumā, tostarp kritisko pakalpojumu darbības nepārtrauktību.

Ar cieņu,

Vitālijs Rakstiņš

UZŅĒMUMU NOTURĪBA UN GATAVĪBA KRĪZĒM

ORGANIZĀCIJAS KRĪZES PĀRVALDĪBAS UN NOTURĪBAS SISTĒMAS IZVEIDE

Organizācijas noturības sistēma balstās uz:

- risku/krīzes pārvaldības sistēmu;
- darbības nepārtrauktības plānošanu;
- piegāžu drošības plānošanu;
- personāla sagatavošanu/apmācībām.

Katram uzņēmumam ir sava risku izvērtēšanas vai krīzes pārvaldības sistēma, tostarp balstoties uz ārējo normatīvo aktu prasībām. Šajā rokasgrāmatā tiks apskatīta uzņēmuma darbības nepārtrauktības plānošana, par pamatu ņemot Ministru kabineta vadlīnijas.
Jāatzīmē, ka darbības nepārtrauktība ir saistīta ar investīcijām un iepirkumiem "miera laikā" – izvēloties drošus, nevis lētākus risinājumus, noturīgus piegādātājus, veidojot krājumus/rezerves un *back up* sistēmas.

RISKU NOVĒRTĒJUMS

Riska pašnovērtējumā ņem vērā visus attiecīgos dabas un cilvēka radītos riskus, kas varētu izraisīt incidentu, tostarp:

- ☑ nelaimes gadījumus;
- ☑ dabas katastrofas;
- ☑ ārkārtas situācijas;
- ☑ hibrīddraudus;
- ☑ cilvēka izraisītus draudus, tostarp teroristu nodarījumus;
- ☑ bezpilota gaisa kuģu draudus;
- ☑ identificēto kritisko izejvielu un materiālu trūkumu, materiāltehnisko resursu nepieejamību un citas konstatētās ievainojamības;
- ☑ militāru apdraudējumu.

RISKU NOVĒRTĒJUMS

Riskus parasti izvieto risku matricā/katalogā atkarībā no to varbūtības un sekām.

Sekas → Varbūtība↓	Maznozīmīgas sekas	Nozīmīgas sekas	Vidējas sekas	Smagas sekas	Katastrofālas sekas
Ļoti augsts					
Augsts					
Vidējs					
Zems					
Ļoti zems					

Sagatavojiet risku pašnovērtējumu un izvietojiet tos risku reģistra tabulā/matricā. Kā var samazināt katra riska iestāšanas varbūtību?

INFRASTRUKTŪRAS FIZISKĀ DROŠĪBA

Infrastruktūras fiziskā drošība ir viens no priekšnosacījumiem vairāku risku novēršanai, tādēļ ir nepieciešams padomāt par ārējā perimetra aizsardzību:

- ☑ žogi un to izvietojums;
- ☑ apgaismojums un tā izvietojums;
- ☑ videonovērošana;
- ☑ citi līdzekļi, kas nodrošina ārējā perimetra aizsardzību vai novērošanu;
- ☑ iekļūšanas kontrole:
  - ☑ apsardzes veids (fiziskā, tehniskā);
  - ☑ iekļūšanas punkti, to izvietojums;
  - ☑ noteiktais caurlaižu režīms darbiniekiem, apmeklētājiem, transportlīdzekļiem un kravām.

Svarīgi, lai ir izstrādāti rīcības algoritmi apdraudējuma un incidentu gadījumā, tostarp attālināti vadāmo ierīču draudu gadījumā.

INFRASTRUKTŪRAS FIZISKĀ DROŠĪBA

Organizācijai ir izstrādāti rīcības algoritmi apdraudējuma situācijās:

- sprādziens;
- bruņots uzbrukums;
- sprādzienbīstama priekšmeta atrašana;
- informācijas saņemšana par spridzināšanas draudiem;
- aizdomīga pasta sūtījuma saņemšana;
- nesankcionēta iekļūšana vai tās mēģinājums;
- nesankcionēta objekta filmēšana, fotografēšana vai cita veida dokumentēšana;
- attālināti vadāmo ierīču iekļūšana objekta teritorijā.

Tālāk sekos piemērs gatavībai noteikta veida apdraudējumam, kā paraugs izmantošanai.

PIEMĒRS, DRONU UZBRUKUMI (SAZIŅA)

PREVENTĪVIE UN GATAVĪBAS PASĀKUMI

- ☑ Sekot līdzi tikai oficiālajai informācijai (VUGD, 112., LSM, NBS vai pašvaldības oficiālajos kanālos);

- ☑ Pārliecināties, ka darbinieku mobilajās ierīcēs ir aktivizēta šūnu apraides paziņojumu saņemšana, kā arī instalēta un darbojas 112 lietotne;

- ☑ Nepieciešamības gadījumā nodrošināt personālu ar telefona modeļiem, kuros ir šūnu apraides iespējas;

- ☑ Pārskatīt un testēt iekšējos saziņas kanālus, kontaktu aktualitāti un informācijas aprites kārtību.

DRONU UZBRUKUMI (DROŠAS TELPAS)

PREVENTĪVIE UN GATAVĪBAS PASĀKUMI

- ☑ Noteikt drošās telpas, ievērojot divu sienu principu. Ja nav pieejamas drošās telpas (divu sienu princips), priekšroka dodama iekštelpām;
- ☑ Nodrošināt skaidru telpu marķējumu (piemēram, marķējumu ar dzeltenu līmlenti ar melnām slīpsvītrām, uzrakstiem "DROŠA VIETA" u.c) un pieejamu informāciju darbiniekiem un apmeklētājiem.
- ☑ Paturēt prātā, ka sprādziena gadījumā īpaši bīstamas ir stikla lauskas, tādēļ, ja telpā ir logi, ir būtiski patverties tieši zem logiem, cieši klāt sienai vai blakus logiem.

DRONU UZBRUKUMI (KONTAKTI)

IEKŠĒJIE PROTOKOLI UN KONTAKTU ĶĒDE

- ☑ Noteikt, kurš saņem informāciju, un kā tā tiek operatīvi nodota tālāk, kā tiek iedarbināti iekšējie protokoli.

- ☑ Pārliecināties, ka kontaktinformācija ir aktuāla.

- ☑ Pirms pasākuma apdraudētā reģionā informēt apmeklētājus/klientus par rīcību brīdinājuma saņemšanas gadījumā un drošās telpas atrašanos (t.sk., ja drošā telpa ir norises telpa, kurā visi atrodas).

- ☑ Noskaidrot apdraudētā reģiona pašvaldības kontaktpersonu (vai komunikācijas kanālu), ar ko sadarboties apdraudējuma gadījumā.

DRONU UZBRUKUMI (ALGORITMI)

Nepieciešams izstrādāt algoritmus rīcībai, ja saņemts šūnapraides brīdinājums par dronu apdraudējumu:

- saņemts darba laikā (vai pasākuma norises vai sagatavošanas laikā);
- saņemts ārpus darba laika.

Papildus nepieciešams plāns:

- ☑ rīcībai ar apmeklētājiem un personām, kas meklē patvērumu pēc paziņojuma saņemšanas;
- ☑ gadījumiem, ja institūcijas teritorijā vai tās tuvumā tiek pamanīts nokritis drons (piemēram, dronam vai tā atliekām netuvoties un tās nepārvietot; nekavējoties atkāpties drošā attālumā; zvanīt 112).

RĪCĪBA ORANŽĀ BRĪDINĀJUMA GADĪJUMĀ

Izstrādāti algoritmi apdraudējuma gadījumā – piemēram, nekavējoties pārtraukt visas aktivitātes (izrādi, koncertu, mācību procesu), kas nenotiek drošās telpās, kurās tiek ievērots divu sienu princips. Var turpināt darboties telpās, kurās tiek nodrošinātas minimālās drošības prasības.

Apzināt klātesošos un organizēt objektā esošo darbinieku un apmeklētāju pārvietošanos uz drošajām telpām, vienlaikus sniedzot informāciju par to, kas notiek; atbildīgajam par informācijas koordinēšanu par apdraudējumu informēt vietējo pašvaldību par to, cik cilvēki ir patvērušies objektā.

Iespēju robežās nodrošināt iespējas cilvēkiem no ārpuses patverties objektā.

Cits piemērs:

AIZDOMĪGU AKTIVITĀŠU PIEMĒRI:

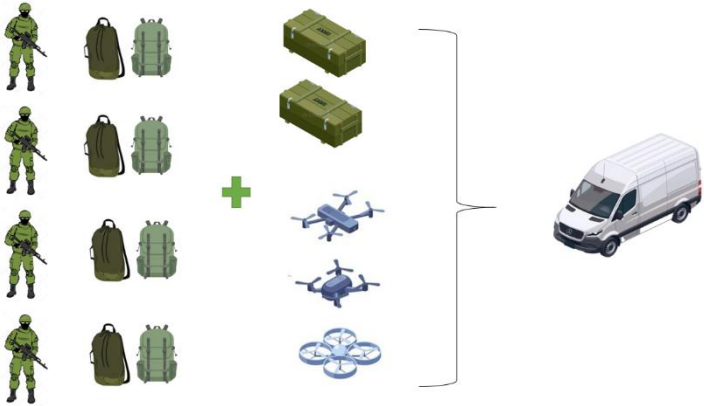
- objekta fotografēšana, filmēšana vai novērošana;
- ilgstoša uzturēšanās objekta tuvumā vai vairākkārtēja pārvietošanās gar to;
- piezīmju veikšana, skicēšana, atrodoties pie objekta;
- mērķtiecīga izvairīšanās no videonovērošanas kamerām;
- piekļūšana objektam tumšajā laikā;
- atzīmju izdarīšana, priekšmetu piestiprināšana vai ierakšana pie objekta vai tā tuvumā;
- aprēķina attālumu līdz objektiem un paziņo koordinātas, objekta azimutu;
- pie objekta novietota kaste, sainis, atkritumu tvertne vai cits priekšmets, kam tur nav jāatrodas.

KĀ ATPAZĪT DIVERSANTUS VAI TERORISTUS?

- fiziski spēcīgi vīrieši vecumā no 18 līdz 45 gadiem;
- 3 līdz 10 cilvēku grupa;
- ir akcents vai arī nemaz nerunā latviešu valodā;
- izvairās no cilvēkiem, ievēro distanci;
- slikti orientējas reģionā;
- aizsedz seju un citādi cenšas slēpt identitāti;
- militāristiem raksturīgi atribūti – kamuflāžas apģērbs, militāra stila zābaki;
- līdzi ir binoklis, nakts redzamības iekārta vai cita novērošanai izmantojama ierīce;
- nestandarta sakaru ierīču, piemēram, rācijas, izmantošana.

KĀ ATPAZĪT DIVERSANTUS VAI TERORISTUS?

Standarta komandā varētu būt 4-5 cilvēki,



kuriem ir:

- vairākas taktiskās mugursomas;
- kastes/lielas somas;
- ieroču somas vai tml.;
- minivens, džips vai mikroautobuss.

KĀ ATPAZĪT DIVERSANTUS VAI TERORISTUS?

Diversantu un teroristu grupas ir atkarīgas no vietējo atbalsta (transports, nauda, informācija u.tml.). Ja identificējat atbalstītājus vai konstatējat kaut ko aizdomīgu, **ziņojiet par to**.

INFORMĀCIJAS DROŠĪBA UN ĢEOTELPISKO DATU KOPAS SLĒPŠANA

Bez liekas vajadzības nevajag eksponēt informāciju par infrastruktūras objektiem:

- ☑ iespēju robežas nodrošiniet kontroli par foto un video uzņemšanu pie objekta un pašā objektā;
- ☑ minimizējiet internetā vai tiešsaistē pieejamo informāciju un datus par infrastruktūru;
- ☑ iespēju robežās veiciet darbības, lai ierobežotu vai vismaz nodrošinātu kontrolētus bezpilota gaisa kuģu lidojumus virs jūsu infrastruktūras (ģeogrāfiskajām zonām).
- ☑ izstrādājiet fotografēšanas/filmēšanas vadlīnijas personālam, ko/kad drīkst fotografēt/publicēt internetā.


BEZ SASKAŅOŠANAS
FOTOGRAFĒT,
FILMĒT
AIZLIEGTS
TĀLRUNIS:_____

IZPLATĪTĀKIE RISKI KORPORATĪVAJĀ VIDĒ

Tieši vai pastarpināti, bet lielākā daļa no iekšējiem riskiem ir **saistīti ar personālu, personāla uzvedību/rīcību vai bezdarbību**

RISKI, KAS SAISTĪTI AR PERSONĀLU

- Apdraudējuma radīšana pārējo darbinieku dzīvībai un veselībai;
- Vadības diskreditēšana;
- Provokācijas;
- Kaitējums organizācijas reputācijai;
- Konfidenciālas informācijas izpaušana;
- Rūpnieciskā spiegošana;
- Zādzība;
- Sabotāža.

Nepieciešamā sistēmiskā pieeja personāla atlasei (pārbaudei) un monitoringam, lai laikus pamanītu jebkādas anomālijas uzvedībā, kas var liecināt par riska iestāšanos.

ANOMĀLIJAS PERSONĀLA UZVEDĪBĀ

Jebkādas anomālijas uzvedībā:

- Konflikti/destruktīva uzvedība vai pašizolācija;
- Nervozitāte, neadekvātas emocionālās reakcijas;
- Fiziskās izmaiņas; pēkšņi parādījies pīrsings, rētas, tetovējumi;
- Būtiski mainījušies vizuālie un lingvistiskie marķieri;
- Neraksturīgas aktivitātes sociālajos tīklos;
- Parādās nauda vai, pretēji - prasa papildu līdzekļus;
- Vairs nestrādā ietekmes/motivācijas rīki.

PAPILDU MARĶIERI/PAZĪMES, KAM SISTĒMISKI PIEVĒRST UZMANĪBU

Darbinieks:

- Regulāri paliek darba vietā pēc darba laika, vakaros/brīvdienās;
- Pēkšņi izrāda pārlieku interesi par jautājumiem, kas nav viņa atbildībā;
- Izvairās no kontaktiem ar uzņēmuma drošības darbiniekiem/IT drošības daļas darbiniekiem;
- Jūtami mainījusies darba produktivitāte/rezultāti;
- Pēkšņa pastiprināta interese par organizācijas datubāzēm/klientu bāzēm;
- Pēdējo mēnešu laikā fiksēti daži drošības instrukciju pārkāpumi.

PERSONĀLA DROŠĪBAS SISTĒMA

Jābūt **sistēmiskai** pieejai:

- ☑ Personāla pārbaudes atlases laikā;
- ☑ Sistēmisks noskaņojumu un uzvedības monitorings;
- ☑ "Nepieciešamības zināt" princips visur;
- ☑ Jauniem darbiniekiem pārbaudes laikā darbs tikai klātienē;
- ☑ Uz risku novērtējumu balstīta elektronisko ierīču izmantošana darbā;
- ☑ Neieinteresētības deklarācijas un interešu konflikta novēršanas sistēma;
- ☑ Skaidra politika par aktivitātēm sociālajos tīklos un par mākslīga intelekta risinājumu izmantošanu;
- ☑ Regulārā apmācība (drošības jautājumi), stress testi, mācības.

KIBERDROŠĪBAS RISKU MAZINĀŠANA

Kiberdrošības riskus var pārvaldīt un samazināt līdz pieņemamam risku līmenim!

Nepieciešams nodrošināt sistēmisku pieeju kiberdrošībai:

- ☑ Korekta iekārtu konfigurācija;
- ☑ Pieejas tiesības (ierobežota piekļuve sistēmām un datubāzēm)
- ☑ Paroles un divu faktoru autentifikācija;
- ☑ Darba attiecību izbeigšanas gadījumā sistēmiskā pieejas liegšana IKT;
- ☑ Mobilo telefonu lietošanas politika;
- ☑ Bring Your Own Device (var/nevar);
- ☑ Datu glabāšanas prasības;
- ☑ Datu pārsūtīšanas nosacījumi;
- ☑ Ārpakalpojumi (gan pieejas tiesības trešajām pusēm; gan trešo pušu IKT izmantošana).

DARBĪBAS NEPĀRTRAUKTĪBA

Darbības nepārtrauktībai nepieciešams:

- ☑ definēt kritiskos pakalpojumus un to minimālo apmēru, kas krīzes laikā jānodrošina vismaz noteiktajā līmenī;
- ☑ identificēt kritisko personālu un tā pienākumus, kā arī personāla sagatavošanas pasākumus;
- ☑ noteikt darbībai nepieciešamo nodrošinājumu (infrastruktūra, tehnoloģiskās iekārtas u.tml.);
- ☑ atrunāt apziņošanu, krīzes komandas aktivizēšanas kārtību/pilnvaras, noteikt rīcības protokolus un krīzes komunikācijas protokolus.

KĀPĒC SVARĪGI ATRAST ALTERNATĪVO LOKĀCIJU?

Krievijas-Ukrainas karš un graujošo tehnoloģiju attīstība ir eksponējusi jaunu infrastruktūras objektu aizsardzības ievainojamību jeb **nevienu infrastruktūras objektu nav iespējams aizsargāt no visiem apdraudējumiem ilglaicīgi**! Tādēļ nepieciešams fokusēties uz kritisko pakalpojumu nepārtrauktību no alternatīvās lokācijas. Iemesli pārcelšanai uz alternatīvo lokāciju var būt arī saistīti ar drošību, piemēram, terorisma draudiem, vai dabas un tehnogēnām katastrofām.

Lai izvairītos no situācijas, kad krīzes laikā jāmeklē alternatīvā lokācija, zvanot vai meklējot internetā, ieteicams apzināšanu veikt jau šodien, neatliekot šo.

DARBĪBAS NEPĀRTRAUKTĪBA

Lai varētu darboties no alternatīvās lokācijas, nepieciešams savlaicīgi:

- ☑ apzināt alternatīvas lokācijas vietas;
- ☑ plānot relokācijas procesu, tostarp personāla un iekārtu pārvietošanu (identificēt nepieciešamo transporta vienību skaitu u.tml.)
- ☑ identificēt iekārtu un materiāltehnisko līdzekļu alternatīvas, remonta iespējas, rezerves daļu pieejamību, atjaunināšanas/uzlabošanas iespēju;
- ☑ nodrošināt IT sistēmu dublēšanu vai restitūciju, lai nodrošinātu pieeju IT sistēmām no citām lokācijām.

AI ALTERNATĪVAJĀ LOKĀCIJĀ IR:

- ☑ sakaru nodrošinājums? alternatīvie sakari?
- ☑ alternatīvie energoapgādes risinājumi?
- ☑ komunālo pakalpojumu pieejamība (ūdens, siltums, kanalizācija u.tml.)?
- ☑ iespējas personāla izmitināšanai?
- ☑ fiziskā apsardze?
- ☑ iespējas piesaistīt vietējo darbaspēku?
- ☑ iespējas veikt iekārtu un ekipējuma remontu vai uzturēšanas darbus?

EVAKUĀCIJA / RELOKĀCIJA

☑ Plānojot evakuāciju, nepieciešamas skaidras vadlīnijas personālam, kā arī iepriekš sagatavotie evakuējamo un iznīcināmo dokumentu saraksti.

Vadlīnijas personālam

Prioritizācija

Dokumentu un datubāžu iznīcināšana

☑ Nepieciešams laicīgi iegādāties kastes, līmi, iesaiņošanas līdzekļus u.tml.

TRANSPORTS

Nepieciešams identificēt un vienoties par:

- ☑ kritisko pakalpojumu sniegšanai nepieciešamo transportu;
- ☑ transporta alternatīvām;
- ☑ autovadītāju un speciālistu pieejamību, aizstāšanas iespējām;
- ☑ nodrošinājumu ar degvielu (vai elektrību, ja ir elektrotransports);
- ☑ atļaujām/licencēm (noteikta veida pārvadājumiem), kā arī noskaidrot, vai transports ir/nav mobilizācijas plānā.

IEKĀRTAS UN MTL

Attiecībā uz kritisko pakalpojumu sniegšanai nepieciešamo tehnoloģisko iekārtu un materiāltehnisko līdzekļu (MTL) risinājumu darbības nepārtrauktības plānā paredz:

- ☑ kritiski svarīgu iekārtu un MTL alternatīvu apzināšanu;
- ☑ nepārtrauktības nodrošināšanu MTL un tehnoloģisko iekārtu zaudējuma vai nedarbošanās gadījumā;
- ☑ rīcību attiecībā uz iekārtu remontu, atjaunošanu, uzlabošanu vai alternatīvu izveidi, ārpakalpojumu nodrošinātāju aizstāšanu;

- ☑ digitālo sistēmu un iekārtu savlaicīgu dublēšanu, lai nodrošinātu pieeju datiem, sistēmām un procesiem arī no alternatīvās lokācijas;

- ☑ piegāžu drošības ietekmi uz iekārtu darbības nepārtrauktību (atbalsta personāla pieejamība, rezerves detaļu pieejamība, remonts);

- ☑ informācijas sistēmu elektroapgādes pieslēguma dublēšanu un aprīkojumu ar autonomu elektroapgādes sistēmu;

- ☑ kritiskā pakalpojuma sniegšanas nepārtrauktības nodrošināšanu alternatīvā veidā ar alternatīviem līdzekļiem.

INFORMĀCIJAS KOMUNIKĀCIJAS (IKT) SISTĒMU DARBĪBAS NEPĀRTRAUKTĪBA

Lai nodrošinātu IKT sistēmu darbības nepārtrauktības plānošanu, var izmantot Ministru kabineta vadlīnijas.[1] Tā, IKT darbības nepārtrauktībai nepieciešams rīcības plāns, kas ietver tīklu, informācijas sistēmu vai to veidojošo elementu darbības nepārtrauktības raksturlielumus (piemēram, atjaunošanas punkta mērķis (RPO), atjaunošanas laika mērķis (RTO), maksimāli pieļaujamais dīkstāves laiks (MTD)), šo raksturlielumu uzraudzības metodiku un rīcības plānu šo raksturlielumu pārsniegšanas gadījumā, tostarp rīcības plānu darbības atjaunošanai nozīmīga kiberincidenta vai krīzes gadījumā.

[1] Ministru kabineta 2025. gada noteikumi Nr. 397 “Minimālās kiberdrošības prasības”.

PERSONĀLS

Lai nodrošinātu kritisko pakalpojumu sniegšanas nepārtrauktību, **nepieciešams**:

- ☑ noteikt kritisko personālu[2];
- ☑ nodrošināt minētā personāla apmācību un sagatavošanu;
- ☑ izstrādāt personāla aizstāšanas un pastiprināšanas kārtību;
- ☑ nodrošināt personālu ar nepieciešamo ekipējumu un aizsarglīdzekļiem;
- ☑ pielāgot infrastruktūru, lai nodrošinātu darbu maiņās, personāla nakšņošanu vai ilgstošu uzturēšanos darba telpās.

[2] Kritiskās infrastruktūras kritiskajam personālam tiek noteikts īpašs statuss un pienākumi, informējot NBS Mobilizācijas struktūras par viņu statusu.

PERSONĀLA DROŠĪBA

Apdraudējuma situācijā, ja darba specifika to ļauj, nepieciešams:

- ☑ nodrošināt attālinātā darba iespējas;
- ☑ pārskatīt uzņēmuma prioritātes, t.sk. apdraudējuma gadījumā uz laiku norīkot dīkstāvē tos darbiniekus, kuri nepilda kritiskās funkcijas (un nevar strādāt attālināti);
- ☑ izmantot darbaspēku ārpus organizācijas (piem., ārpakalpojumu);
- ☑ automatizēt procesus, pārskatīt procesus un, kur iespējams, ieviest pašapkalpošanās platformas/kioskus.

PERSONĀLA UZTURĒŠANĀS DARBĀ

Lai nodrošinātu darbu maiņās, nakšņošanu vai ilgstošu uzturēšanos darba telpās, nepieciešamas:

- ☑ gultas vietas;
- ☑ pārtikas krājumi un ūdens pieejamība;
- ☑ pirmās nepieciešamības preču krājumi u.tml.
- ☑ 72 stundu gatavības somas.

PERSONĀLA PSIHOLOĢISKĀ SAGATAVOTĪBA

Krievijas-Ukrainas kara pirmajās dienās tika īstenotas psiholoģiskās iebiedēšanas operācijas, tostarp zvanot un draudot ukraiņu amatpersonām un viņu ģimenes locekļiem.

Nepieciešams:

- ☑ sagatavot personālu šādām situācijām;
- ☑ izstrādāt rīcības algoritmus;
- ☑ apmācīt arī ģimenes locekļus.

PERSONĀLA NODROŠINĀJUMS

- ☑ Darba uzdevumu izpildei personālu jānodrošina ar aizsarglīdzekļiem, nepieciešamo ekipējumu un MTL;

- ☑ Ņemot vērā, ka privātajam sektoram ir noteikti ierobežojumi divējādā lietojuma preču iegādei (piemēram, noteiktas klases bruņuvestes vai aizsargķiveres), personālu būtu vērts nodrošināt vismaz ar darba aizsardzības specializēto ekipējumu un individuāliem aizsardzības līdzekļiem.

ĀRĒJIE (KRITISKIE) PAKALPOJUMI

Darbības nepārtrauktības plānā nepieciešams atrunāt alternatīvus risinājumus:

- ☑ elektroniskajiem sakariem un balss telefonijai;
- ☑ elektroenerģijas apgādei;
- ☑ pieejai internetam;
- ☑ pieejai finanšu pakalpojumiem;
- ☑ dabasgāzei un naftas produktiem;
- ☑ apkurei, ūdensapgādei, kanalizācijai;
- ☑ loģistikas risinājumiem.

SAKARI

Nepieciešams veidot sistēmu, kad organizācijā vienlaikus ir primārie, alternatīvie un ārkārtas sakari:

- ☑ mobilie sakari un internets;
- ☑ MS Teams vai līdzīgi risinājumi;
- ☑ saziņas lietotnes (Signal, WhatsApp);
- ☑ fiksētas/analogas telefona līnijas;
- ☑ satelīta sakari/Starlinks u.tml.

ELEKTROENERĢIJA

Elektroapgādes pārtraukumi ietekmē visus uzņēmuma procesus, tādēļ viena no pamata prasībām darbības nepārtrauktībai ir alternatīvi elektroenerģijas piegādes risinājumi[3].

Uzņēmumi var izmantot 2025. gada februāra pieredzi, gatavojoties elektroenerģijas atslēgšanai no Krievijas tīkla (BRELL).

---

[3] Ministru kabineta 2024. gada 27. augusta noteikumi Nr. 576 "Enerģijas lietotāju apgādes kārtība izsludinātas enerģētiskās krīzes laikā un valsts apdraudējuma gadījumā" nosaka, ka kritiskai infrastruktūrai ir pienākums pastāvīgi nodrošināt sev individuālās elektroenerģijas apgādes iespēju, ja valsts apdraudējuma vai valsts enerģētiskās krīzes laikā tiek pārtraukta elektroenerģijas piegāde.

ELEKTROENERĢIJA

Nepieciešams:

- ☑ savlaicīgi vienoties ar komersantiem, kuri var nodrošināt alternatīvu (elektroenerģijas dīzeļģeneratorus)[4];
- ☑ iegādāties rezerves ģeneratorus/ modernizēt esošus;
- ☑ sadarbībā ar citiem infrastruktūras īpašniekiem kopīgi iegādāties un uzturēt dīzeļģeneratoru(s).

[4] [!] Jāskatās uz šī ārpakalpojuma - dīzeļģeneratora piegādi – piegādes nosacījumiem, jo krīzē ģeneratorus vienlaikus pieprasīs visi klienti, attiecīgi, vai ir garantija, ka tieši jūsu organizācijai tas tiks piegādāts.

KRITISKIE FINANŠU PAKALPOJUMI

AS "Swedbank", AS "SEB banka", AS "Citadele banka" un Luminor Bank AS Latvijas filiālei apdraudējuma gadījumā jānodrošina:

- bezskaidras naudas maksājumu pakalpojumu pieejamība noteiktā apmērā;
- maksājumu veikšana ar maksājumu karti, t.sk. maksājumu veikšana tiešsaistē, ja nav traucēta starptautisko karšu shēmu vai norēķinu starpnieku infrastruktūras darbība;
- skaidras naudas nepārtraukta pieejamība jānodrošina vismaz 10 procentu apmērā skaidras naudas izmaksas punktos (bankomātos).

KRITISKIE BANKOMĀTI

Latvijā ir izveidota sistēma ar kritiskiem kredītiestāžu bankomātiem, kuri jebkurā apdraudējuma situācijā prioritāri tiek apgādāti ar skaidro naudu. Latvijas Bankas tīmekļa vietnē ir pieejama interaktīva karte: https://www.bank.lv/pakalpojumi/bankomatu-karte Iepazīsties šodien, kur ir tuvākie kritiskie bankomāti.

Situācijā, ja maksājumu karšu infrastruktūra nav pieejama, bankas nodrošina vismaz tādu maksājumu karšu, kas izsniegtas fiziskām personām un aprīkotas ar kontakta mikroshēmām, pieņemšanu Latvijas Republikā, izmantojot bezsaistes risinājumu.

Citiem vārdiem – ja nav pieejams internets, pastāv iespējas veikt maksājumus ar Latvijā izsniegto karti līdzīgi, kā to var izdarīt lidmašīnās.

Izmantojot bezsaistes risinājumu, bankām jānodrošina iespēja iegādāties **pirmās nepieciešamības preces** par kopējo summu, kas nepārsniedz 200 euro. Tāpat tiek strādāts pie risinājumiem, lai uzņēmumi arī spētu veikt savstarpējos maksājumus bezsaistē.

PIEGĀŽU DROŠĪBA UN NOTURĪBA

Lai nodrošinātu piegāžu noturību un nepārtrauktību arī militārā apdraudējuma gadījumā, **nepieciešams miera laikā jeb jau šodien**:

- ☑ sadalīt piegāžu riskus (*multi vendor suppliers*), izvairoties no atkarības tikai no viena piegādātāja;
- ☑ izvairīties no augsta riska piegādātāju (KTR, Krievija, Baltkrievija u.c.) iesaistes piegāžu ķēdēs;
- ☑ laikus apzināt alternatīvās piegāžu ķēdes vai alternatīvu kritiskajām izejvielām, produktiem, MTL un pakalpojumiem;

- ☑ iespēju robežās glabāt kritiskās izejvielas un produkcijas rezerves jeb īstenot *just in case* biznesa modeli;

- ☑ prioritāri iesaistīt vietējās piegāžu ķēdes un vietējos uzņēmumus.

Netiek rekomendēts izmantot tādu uzņēmumu ražotās tehnoloģijas, kuru reputācija Eiropas Savienības un NATO dalībvalstīs tiek apšaubīta saistībā ar aizdomām par informācijas nesankcionētu iegūšanu, privātuma pārkāpumiem vai valsts drošības apdraudējumu.

MILITĀRAIS APDRAUDĒJUMS

IZŅĒMUMA STĀVOKLIS

Kad iestājas stunda X? Stunda X iestāsies no brīža, kad Ministru kabinets izsludinās speciālo tiesisko režīmu izņēmuma stāvokli.

Izņēmuma stāvokli izsludina valsts militārā apdraudējuma gadījumā:

- kad valsti apdraud ārējais ienaidnieks, vai
- valstī vai tās daļā ir izcēlušies vai draud izcelties iekšēji nemieri, kas apdraud demokrātisko valsts iekārtu.

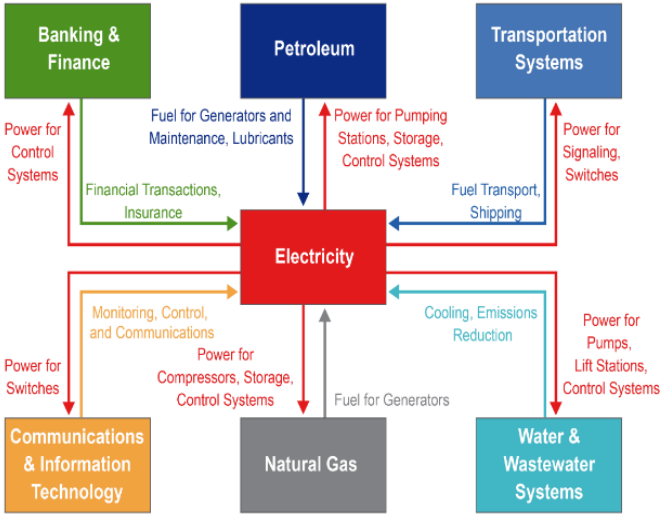
Izņēmuma stāvokļa izsludināšanas gadījumā uzņēmumam ir nepieciešams aktivizēt krīzes komandas, rīcības protokolus un darbības nepārtrauktības plānus apdraudējuma gadījumam.

KRITISKĀS FUNKCIJAS

Normatīvie akti uzdod par pienākumu nodrošināt kritisko funkciju darbības nepārtrauktības īstenošanu vismaz minimālā apjomā izņēmuma stāvokļa laikā.

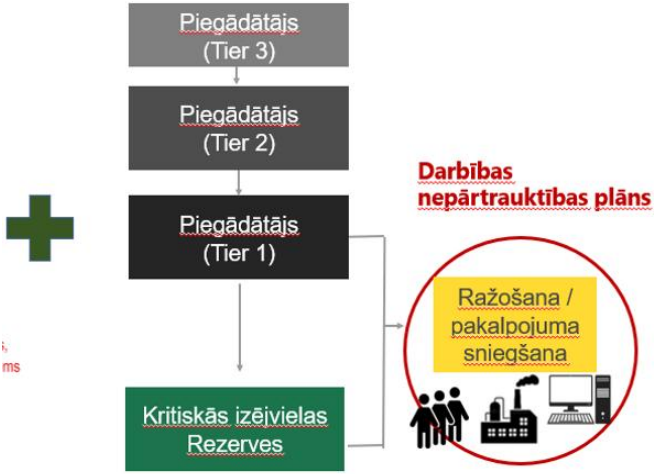
Likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" 17. panta pirmās daļas 24) punkts nosaka aizliegumu juridiskajām personām pārtraukt kritiskās infrastruktūras vai kritisko finanšu pakalpojumu darbību izņēmuma stāvokļa laikā (pienākums strādāt un nodrošināt valstij un sabiedrībai kritiskās funkcijas vismaz minimālā apmērā). Kopš 2021. gada visiem kritisko pakalpojumu komersantiem ir noteikts pienākums turpināt strādāt kara laikā jeb ir plānošanas pieņēmums un savstarpējā paļaušanās, ka tiks nodrošināti visi pārējie kritiskie pakalpojumi.

KĀ NODROŠINĀT KRITISKO FUNKCIJU DARBĪBAS NEPĀRTRAUKTĪBU?



Izaicinājums: visi kritiskie pakalpojumi ir savstarpēji saistīti un atkarīgi viens no otra.

Tādēļ tiek strādāts vienlaikus ar visu nozaru kritisko pakalpojumu sniedzējiem, lai pilnīgi visas kritiskās funkcijas tiktu nodrošinātas.



VAI IR IESPĒJAMS AIZSARGĀT OBJEKTU KARA LAIKĀ?

Pirmā līmeņa aizsardzība ir infrastruktūras inženiertehniskās aizsardzības elementu kopums, kas nodrošina pasīvo aizsardzību:

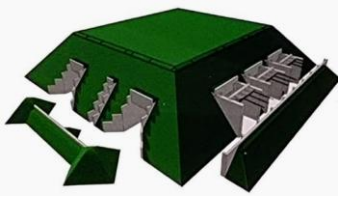
- ☑ Pasīvās barjeras, aizsargvaļņi, betona bloki;
- ☑ Smilšu maisi un HESCO bastioni;

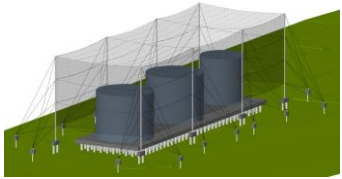
- ☑ Ekipējuma un ražošanas iekārtu decentralizācija objekta teritorijā;
- ☑ Maskēšanas pasākumi, lai grūti identificēt vērtīgākos resursus;

- ☑ Iespēju robežās izvietojot svarīgākās/ vērtīgākās iekārtas un MTL pagrabtelpās vai pazemē;
- ☑ Aizlīmēt/aiznaglot logus;

- ☑ Atbrīvot telpas ar logiem no nevajadzīgiem priekšmetiem, kas sprādzienā var savainot personālu;
- ☑ Taktiskie tīkli un pretdronu aizsardzības konstrukcijas;
- ☑ Pretdronu sensori un radari, kameras/ infrasarkanie sensori; audio sensori;
- ☑ Dažādas civilajam sektoram pieejamas iekārtas pretdarbībai bezpilota platformām.

Otrā līmeņa aizsardzību var nodrošināt tikai ar nopietniem inženiertehniskiem darbiem, būvējot metālisko tīklu konstrukcijas vai pat betona sienas apkārt objektam, vai ievietojot svarīgākās iekārtas betona sarkofāgā.





Trešā līmeņa aizsardzība ir daudzslāņaina pretgaisa infrastruktūras aizsardzība, kas ietver vairāku veidu pasīvās un aktīvās pretdronu sistēmas:

- ☑ sensoru un radaru tīkli;
- ☑ siltumvizori, video kameras, prožektori un citas ierīces dronu identifikācijai;

- ☑ pretdronu elektromagnētiskie ieroči, slāpētāji, lāzeri un citi ieroči dronu notriekšanai taktiskajā līmenī;
- ☑ mobilās pretgaisa / pretdronu grupas.

PRETGAISA/PRETDRONU AIZSARDZĪBA

Pēdējie grozījumi[5] atļāva kritiskās infrastruktūras drošības dienestiem vai apsardzes komersantiem pretdarboties bezpilota platformām (gaisa, ūdens/ zemūdens; sauszemes). Tomēr komersantiem ir ierobežotas iespējas iegādāties jaudīgos slāpētājus vai divējāda lietojuma ieročus; otrkārt, to pielietošana ir ierobežota (t.sk. sistēmas "savs-svešs" nepieciešamības dēļ, lai novērstu draudzīgu dronu notriekšanu). Tādēļ ir nepieciešama cieša sadarbība ar drošības dienestiem. Ilgtermiņā ir jādomā par vienotas novērošanas sistēmas/tīkla izveidi kritiskajai infrastruktūrai, lai katrai organizācijai nebūtu jāveido savas autonomās spējas.

[5] Nacionālās drošības likumā un Apsardzes darbības likumā.

APSARDZE

Kritisko pakalpojumu nodrošināšana nav iespējama bez apsardzes, tādēļ arī apsardzes funkcijas tiek atzītas par kritiskajām.

Ukrainā identificēti šādi izaicinājumi:

- ☒ apsardzes darbinieku mobilizācija;
- ☒ inkasācijas transporta rekvizīcija;
- ☒ augsti riski apsardzes darbībai.

Daži risinājumi Ukrainā:

- ☑ apsargu atbrīvojums no mobilizācijas;
- ☑ sieviešu iesaiste apsardzes darbībā.

News

Banks are forced to close a third of branches due to fighting

Friday, March 25, 2022 08:30

News

The war made cash collection very difficult

Friday, March 25, 2022 10:00 a.m

BUMBU PATVERTNES PERSONĀLAM

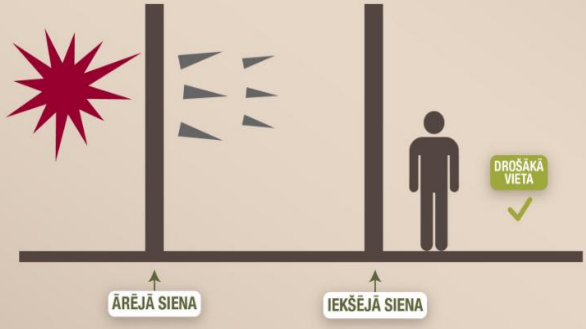
- ☑ Nepieciešams apzināt tuvumā esošās patvertnes vai apsvērt tādus alternatīvus risinājumus kā mobilās patvertnes;

- ☑ Ja iespējams, ir jāapsver iespēja atjaunot patvertnes objektos (ja bija);

- ☑ Nepieciešams pielāgot iekštelpas, identificējot telpas vismaz divu sienu attālumā no ārsienas, jo tas sniegs papildu aizsardzību un pasargās no triecienviļņa un šķembām.

Iekštelpās ievēro “vismaz divu sienu” principu – meklē patvērumu aiz divām sienām. Aizver logus un durvis, netuvojies tiem. Tas sniedz papildu aizsardzību un pasargā no triecienviļņa un šķembām.

Ja nav iespējams ievērot divu sienu principu, paliec iespējami tālāk no logiem.



PIENĀKUMS STRĀDĀT KARA LAIKĀ

Valsts apdraudējuma gadījumā izsludināta izņēmuma stāvokļa laikā kritiskais personāls:

- ☒ nav pakļauts mobilizācijai*;
- ☒ nevar uzteikt darba līgumu**;
- ☒ nevar pārtraukt tiešo darba pienākumu pildīšanu, izņemot gadījumus, kad tas apdraud dzīvību.

* Mobilizācijas likuma 14.[1] pants.

** Likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" 17. panta pirmās daļas 23) punkts.

MOBILITĀTE

Atkarībā no apdraudējuma kritiskais personāls var īstenot drošības algoritmus, visu laiku mainot uzturēšanās lokāciju un mainīt nakšņošanas vietas. Piemērs ar Ukrainas aizsardzības ministru Reznikovu kara sākumā.

Lai īstenotu līdzīgus drošības pasākumus, organizācijai nepieciešamas transporta spējas mobilitātei un virkne alternatīvu lokāciju.

RĪCĪBAS ALGORITMU IZSTRĀDE

(piemērs, rīcība apšaudes gadījumā):

- Operatīvā apziņošana un evakuācija uz bumbu patvertnēm;
- Iespēju robežās – iekārtu atslēgšana (lai minimizētu zaudējumu apmēru);
- Objekta taktiskie aizsardzības pasākumi, primāri sensitīvā ekipējuma aizsardzība pret šķembām u.tml;
- Ugunsdzēsēju brigāžu atrašanās netālu no objektiem (10-15 min braukšanas attālumā), jo savlaicīga iesaiste seku likvidācijā minimizē zaudējumus;
- Remonta spēju/brigāžu sagatavošana, nodrošinot tās ar transportu, degvielu, aizsargekipējumu.
- Rezerves detaļu uzglabāšana un kanibalizācijas opciju apzināšana (no citiem objektiem).

GALVENIE IZAICINĀJUMI, AR KURIEM SASKĀRUSIES UZŅĒMUMI UKRAINĀ:

[1] Personāla un ģimenes drošība;
[2] Pieprasījuma/pirktspējas samazināšanās;
[3] Piegādes ķēžu traucējumi/pārrāvumi;
[4] Izaicinājumi ar loģistiku (just in time);
[5] Finansējuma/kredītu nepieejamība;
[6] Izejvielu, materiālu un enerģijas izmaksas;
[7] Kvalificēta darbaspēka trūkums;
[8] Sakaru/interneta traucējumi;
[9] Elektroenerģijas piegādes traucējumi;
[10] Komunālo pakalpojumu nenodrošināšana
[11] Komandantstunda (darbs nakts stundās);
[12] Priekšapmaksa visur;
[13] Infrastruktūras iznīcināšana/bojāšana;
[14] Kiberuzbrukumu skaita pieaugums;
[15] Ilgtermiņa projektu apturēšana;
[16] Personāla un transporta mobilizācija;
[17] Izceļošanas ierobežojumi.

NEPIECIEŠAMAIS ATBALSTS NO VALSTS

Nepieciešamais atbalsts no valsts institūcijām, lai nodrošinātu kritisko funkciju īstenošanu:

- ☑ prioritārais nodrošinājums ar energoresursiem, gāzi un degvielu;
- ☑ sakaru nodrošinājums;
- ☑ fiziskā apsardze/kiberaizsardzība;
- ☑ loģistikas atbalsts;
- ☑ atvieglojumi, izņēmumi, atļaujas, papildu tiesības;
- ☑ cits atbalsts krīzes laikā.

Daži piemēri no Ukrainas:

- kritiskā personāla **atbrīvojums** no mobilizācijas uz pusgadu;
- prioritārais nodrošinājums ar resursiem (piemēram, degvielas deficīta gadījumos);
- nepieciešamo atļauju piešķiršanu būvniecībai paātrināšana;
- nepieciešamo licenču un atļauju izsniegšana, darbības pagarināšana;
- radio frekvenču (piemēram, 2100 MHz joslā piešķiršana lielākajiem operatoriem, lai palielinātu 3G/4G tīklu jaudu un uzlabotu radio pārklājumu.

KOPSAVILKUMS

- Infrastruktūru nav iespējams aizsargāt no visiem apdraudējumiem ilglaicīgi! Daudzi riski ir jāakceptē!

- Bez kinētiskas un digitālās drošības ir nepieciešams fokusēties uz kritisko pakalpojumu nepārtrauktību.

- Nepieciešams veidot spējas, kas nav balstītas tikai uz riskiem (risku apetīti, risku reģistru), bet veidot arī iekšējās spējas/rezerves, lai spētu funkcionēt jebkādā krīzē.

- Kritiski svarīga valsts / regulatoru koordinējošā loma, ņemot vērā kritisko pakalpojumu savstarpējās atkarības un kaskadējošos efektus.

TRĪS LIETAS, KO MANA ORGANIZĀCIJA / UZŅĒMUMS VAR IZDARĪT, LAI BŪTU NOTURĪGA KRĪZES SITUĀCIJĀS?

[1] iespēju robežās **izstrādāt darbības nepārtrauktības plānu** atbilstoši Ministru kabineta rekomendācijām[6]

[2] **piegāžu drošība**: iespēju robežās izveidot un uzturēt kritisko izejvielu, preču un rezerves daļu krājumus (just in case biznesa modelis) un diversificēt piegāžu avotus, un, ja tas

[6] Ministru kabineta 2026. gada 13. janvāra noteikumi Nr. 10 "Kritiskās infrastruktūras apzināšanas, darbības nepārtrauktības, drošības un noturības pasākumu plānošanas, īstenošanas un incidentu paziņošanas kārtība" (1.pielikums) un Ministru kabineta 2025.gada noteikumi Nr.397 "Minimālās kiberdrošības prasības" (9.pielikums).

iespējams, prioritāti liekot uz vietējiem ražotājiem un piegādātājiem; neskatīties uz saimnieciski izdevīgākiem piedāvājumiem, bet noturīgākiem risinājumiem;

[3] **apmācīt** personālu rīcībai krīzes situācijās, regulāri **organizēt stresa testus un krīzes situāciju simulācijas**.

Daļa no rekomendācijām prasa nopietnu resursu ieguldīšanu, daļa neprasa, tomēr uzņēmumu noturība un spēja turpināt darboties krīzē ir nozīmīga tautsaimniecībai, jo katrs komersants, kas spēj funkcionēt krīzē, ar šo funkcionalitāti jau sniedz atbalstu nacionālajai drošībai.