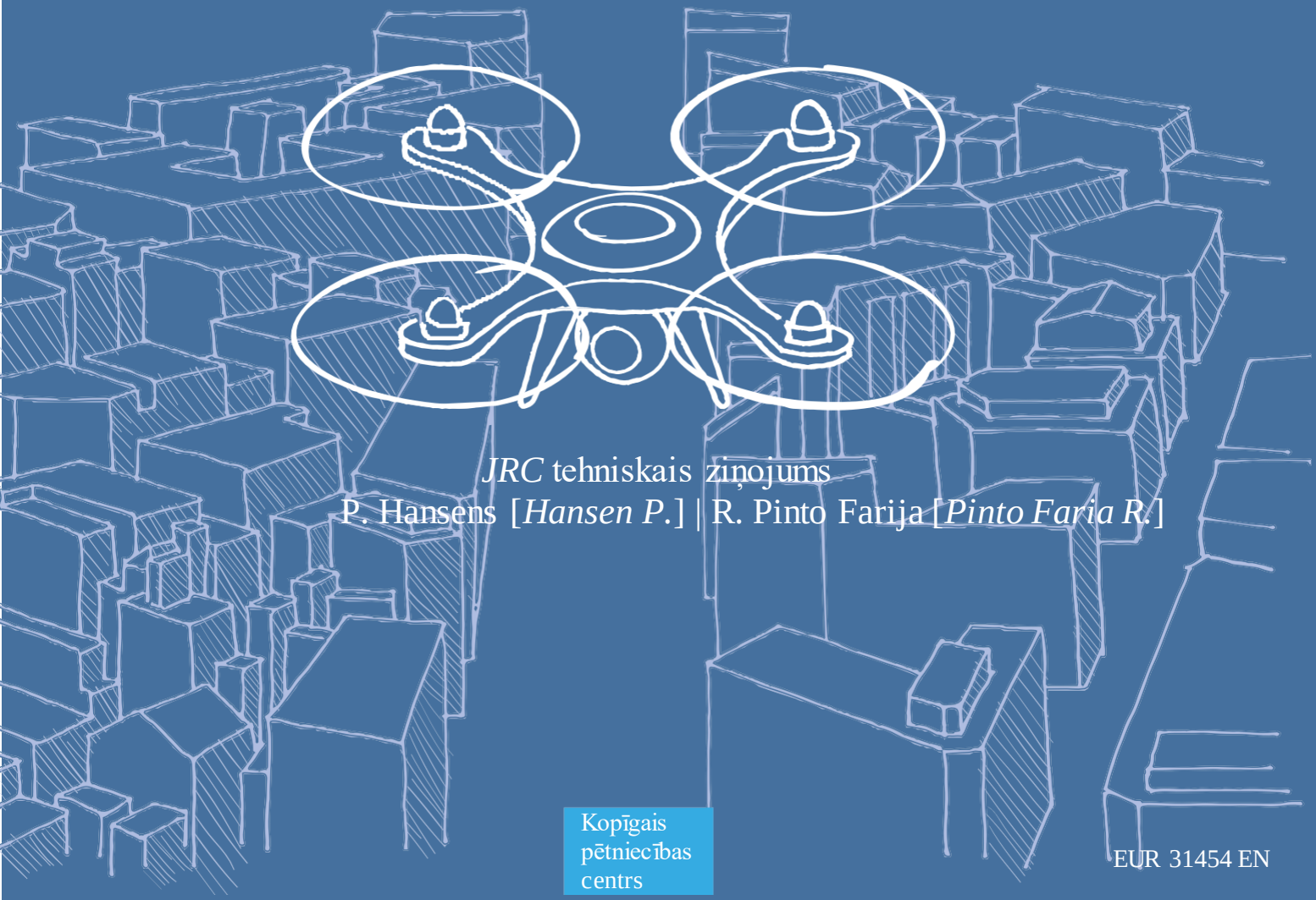
ISSN 1831-9424

European Commission

Aizsardzība pret bezpilota lidaparātu sistēmām

Rokasgrāmata par kritiskās infrastruktūras un sabiedrisku vietu aizsardzību pret *UAS* Piecu posmu pieeja *C-UAS* ieinteresētajām personām



JRC tehniskais ziņojums

P. Hansens [*Hansen P.*] | R. Pinto Farija [*Pinto Faria R.*]

Kopīgais pētniecības centrs

EUR 31454 EN

Šī publikācija ir Eiropas Komisijas zinātnes un zināšanu dienesta Kopīgā pētniecības centra (*JRC*) tehniskais ziņojums. Tas izstrādāts, lai ar pierādītu zinātnisko pamatojumu palīdzētu veidot Eiropas politiku. Šīs publikācijas saturs ne vienmēr atspoguļo Eiropas Komisijas viedokli vai nostāju. Komisija un citas personas, kas rīkojas Komisijas vārdā, neatbild par šīs publikācijas izmantošanas veidu. Lai iegūtu informāciju par šajā publikācijā izmantoto datu, kuru avots nav ne *Eurostat*, ne citi Komisijas dienesti, piemēroto metodiku un kvalitāti, lietotājiem jāsazinās ar norādīto datu avotu. Šajā izdevumā lietotie apzīmējumi un informācijas izklāsts par kartēm neatspoguļo Eiropas Savienības viedokli par kādas valsts, teritorijas, pilsētas vai rajona vai to pārvaldes iestāžu juridisko statusu, ne arī par to robežu norobežošanu.

Kontaktinformācija

Vārds, uzvārds: Pauls HANSENS (*HANSEN Paul*) (*JRC-GEEL*)
Adrese: Eiropas Komisija
Joint Research Centre
Retieseweg 111
2440 Geel
BELGIQUE/BELGIË

Tālr.: +32 (0)14 571 485
E-pasta adrese: JRC-DRONE@ec.europa.eu

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC132714
EUR 31454 EN

Iespiedums	*ISBN* 978-92-68-06614-0	ISSN 1018-5593	doi:10.2760/747997	KJ-NA-31-454-EN-C
PDF	*ISBN* 978-92-68-01253-6	ISSN 1831-9424	doi:10.2760/18569	KJ-NA-31-454-EN-N

Luksemburga: Eiropas Savienības Publikāciju birojs, 2023. gads

Kā citēt šo ziņojumu: Hansen, P., Pinto Faria, R., Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/18569, JRC132714.

Aizsardzība pret bezpilota lidaparātu sistēmām

Rokasgrāmata par kritiskās infrastruktūras un sabiedrisku vietu aizsardzību pret *UAS* Piecu posmu pieeja *C-UAS* ieinteresētajām personām

JRC tehniskais ziņojums

P. Hansens [*Hansen P.*] | R. Pinto Farija [*Pinto Faria R.*

Saturs

Kopsavilkums

Lai izstrādātu efektīvu bezpilota lidaparātu sistēmu apkarošanas (*C-UAS*) risinājumu un saskaņotu procesus un procedūras, jāsadarbojas daudzām ieinteresētajām personām. Šo rokasgrāmatu izstrādāja Eiropas Komisijas Kopīgais pētniecības centrs (*JRC*), un tajā izmantota pieredze, kas gūta, īstenojot *DRONE* projektu[1]. Ieteikumi ir izstrādāti, īstenojot sadarbības projektu. Šajā rokasgrāmatā iekļautie ieteikumi ir izstrādāti pēc mērķtiecīgas apspriešanās un darbseminmāriem, kur piedalījās tādas galvenās ieinteresētās personas kā tiesībaizsardzības iestādes (*LEA*), iestādes, regulatīvās iestādes un tehnoloģiju uzņēmumi.

Rokasgrāmatā ir sniegti ieteikumi aizsardzībai pret ļaunprātīgi izmantotām *UAS*, kā arī norādījumi, norādes, metodes un apsvērumi. Tajā aplūkota *UAS* izsekošana, identificēšana un neitralizēšana, izpildot riska analīzes procedūras, izstrādājot risinājumu, ieviešot to un nodrošinot tā darbību. Rokasgrāmatā izskaidrots, cik svarīgi ir apvienot sistēmas un procesus, iesaistot ieinteresētās personas, lai izveidotu pilnīgu risinājumu.

Šī rokasgrāmata ir galvenais elements Komisijas *C-UAS* pakotnē, kas kā pamatdarbība izziņota Komisijas paziņojumā "Dronu stratēģija 2.0 viedai un ilgtspējīgai bezpilota gaisa kuģu ekosistēmai Eiropā"[2]. Šajā pakotnē ir *C-UAS* veltīts paziņojums, kurā izklāstītas galvenās ierosmes ES turpmākajai politikai attiecībā uz potenciālā *UAS* radītā apdraudējuma novēršanu. Iesaistoties centienos sniegt pastāvīgu praktisku atbalstu ES dalībvalstīm un ieinteresētajām personām, *JRC* ir izstrādājis divas rokasgrāmatas. Pirmajā aplūkota šī piecu posmu pieeja, ko izmantot, lai izstrādātu *C-UAS* risinājumu, bet otrā rokasgrāmatā ir sniegta virkne ieteikumu attiecībā uz tādu risku novērtēšanu, kurus rada ļaunprātīga *UAS* izmantošana, pievienojot ieteikumus par nemilitāru infrastruktūru nostiprināšanu pret šādiem apdraudējumiem.

[1] EU Science Hub, https://joint-research-centre.ec.europa.eu/scientific-activities-z/drones-counter-drones-and-autonomous-systems_en.

[2] Komisijas paziņojums – Dronu stratēģija 2.0 viedai un ilgtspējīgai bezpilota gaisa kuģu ekosistēmai Eiropā, COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52022DC0652.

Ievads

Eiropā un pārējā pasaulē aizvien vairāk izmanto *UAS* (ko parasti dēvē par droniem). Lai paplašinātu *UAS* izmantošanu tādās nozarēs kā lauksaimniecība, transports, uzraudzība un novērošana, ir definēti vispārējie *UAS* pakalpojumi[3], skat. 1. attēlu. ES drošuma satvars attiecībā uz bezpilota lidaparātu ekspluatāciju un tehnisko prasību noteikšanu saskaņo Eiropas *UAS* tirgu, un tam jāuzlabo *UAS* izmantošana un ar to saistītā izstrāde un pakalpojumi.

Lai gan *UAS* piedāvā vērtīgas iespējas komerciālai izmantošanai, pastāv iespēja tās izmantot arī ļaunprātīgi. *UAS* var izmantot, lai pārkāptu privātuma noteikumus, spiegotu, izmantojot videokameru tehnoloģijas, uzlauztu telesakaru signālus un, aprīkotas ar bioloģiskām vai ķīmiskām vielām, sprāgstvielām vai citiem ieročiem, tās var apdraudēt cilvēkus, traucēt pakalpojumu sniegšanu un sagraut infrastruktūru.

Lai gan vairākumā gadījumu nesadarbīga *UAS* izmantošana, iespējams, būs neapzināta (nevērīga un nezinoša), nevar izslēgt, ka noziedznieki un teroristi aizvien biežāk *UAS* varētu izmantot ļaunprātīgi, lai veiktu uzbrukumus sabiedriskām vietām, cilvēkiem un kritiskai infrastruktūrai (KI). Šāda tendence, kad *UAS* izmantotas teroristu uzbrukumos, jau ir novērota visā pasaulē. Tā kā *UAS* incidentu darbības veidi un mērķi ir bijuši tik ļoti atšķirīgi, pretpasākumos ir jāiekļauj kā aktīvie, tā pasīvie elementi.

Lai gan, pateicoties ES noteikumiem, *UAS* izmantošana ir kļuvusi drošāka un vienlaikus ir apgrūtināta ļaunprātīga noteiktu veidu *UAS* izmantošana, straujais inovācijas temps un vieglā piekļuve *UAS* nozīmē to, ka incidenti, visticamāk, notiks aizvien biežāk. Tā kā šādu incidentu biežums un ietekme pieaug[4], kritisko infrastruktūru īpašniekiem un sabiedrisko vietu pārvaldniekiem ir jo īpaši svarīgi ieviest preventīvus pretpasākumus un būt gataviem.

Tirdzniecībā ir pieejamas daudzas *UAS* un to sastāvdaļas, ko var pārveidot izmantošanai konkrētā ļaunprātīgā nolūkā. Tādēļ ir nepieciešami pretpasākumi, lai kontrolētu nesadarbīgu vai ļaunprātīgu *UAS* izmantošanu.

[3] https://www.sesarju.eu/U-space.
[4] https://transport.ec.europa.eu/system/files/2022-11/SWD_2022_366_drone_strategy_2.0.pdf

Šīs rokasgrāmatas piemērošanas joma un mērķis

Šis ir pirmais rokasgrāmatas izdevums, ko var uzskatīt par dinamisku dokumentu, kas aptver jomu, kura strauji attīstās. Komisija rūpīgi uzraudzīs attiecīgās norises regulatīvajā, procesuālajā un tehniskās attīstības jomā un nākamajos gados vajadzības gadījumā atjauninās rokasgrāmatu.

1. attēls. Kritiskās infrastruktūras veidi, par kuriem sniegti ieteikumi šajā rokasgrāmatā

Angļu val.	Latviešu val.
Energy	Energoapgāde
Border	Robežas
Food	Pārtika
Harbour	Osta
Transport	Transports
Airport	Lidosta
Chemical	Ķīmiskā viela
Health	Veselība
ICT	IKT
Financial	Finanses
Public spaces	Sabiedriskas vietas
Space and research	Kosmoss un pētniecība
Water	Ūdens
Public and legal order, safety	Sabiedriskā un tiesiskā kārtība, drošums

Šajā rokasgrāmatā nav iekļauts plašs pārskats par pieejamām *C-UAS* metodēm un tehnoloģijām. Toties tajā ir izklāstīta metodika un ieteikumi attiecībā uz nepieciešamā *C-UAS* risinājuma izvēli, tā izstrādi un ieviešanu. Rokasgrāmatā ir sniegti norādījumi par vispiemērotākā risinājuma noteikšanu un piedāvāta pieeja šāda risinājuma ieviešanai un izmantošanai.

Lai gan risinājumi ir diezgan līdzīgi, ir skaidrs, ka nav viena *C-UAS* risinājuma, kas būtu piemērots visos gadījumos, un ka vienādi risinājumi nebūs iespējami. Šeit izklāstītie ieteikumi

ir pietiekami vispārīgi, lai tos varētu izmantot kā pienācīgu pamatu tādu nākamo risinājumu izstrādei, kuri šobrīd vēl nepastāv.

Sākuma, izstrādes un uzstādīšanas posmi tika izmēģināti un pārbaudīti projektā, īstenojot *JRC DRONE* projekta koncepcijas apliecinājuma daļu, kurā bija iekļauta dzīvā laboratorija *JRC* Gēlas mītnē. Ieteikumi attiecībā uz uzstādīšanas un darbības posmiem ir pamatoti ar kopējiem projekta un risinājuma īstenošanas principiem. Rokasgrāmatas ieteikumi ir pamats *C-UAS* dzīvajai laboratorijai, kas būs pieejama ieinteresētajām personām, lai noteiktu regulējuma vajadzības, organizētu procesus un procedūras un optimizētu *C-UAS* risinājumus.

Piecu posmu pieeja C-UAS risinājumam

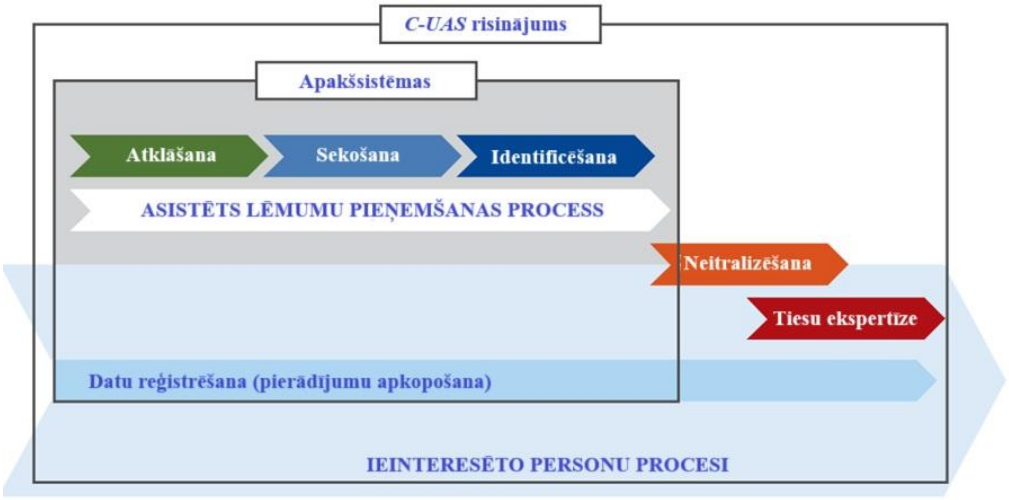
C-UAS noteikti ir sarežģīts uzdevums, un nav iespējams ieviest risinājumu, kas būs piemērots visām situācijām, tāpēc, visticamāk, nebūs standartizētu ieviešanas paņēmienu vai identisku risinājumu. Ikviens risinājums būs jāpielāgo atbilstīgi konkrētā objekta un tā vides vajadzībām. Tomēr ir arī kopīgi elementi, un visos ieviešanas gadījumos būs lietderīgi izmantot šajā dokumentā izklāstītos ieteikumus.

Lai gan parasti *C-UAS* ietver atklāšanu, izsekošanu, identificēšanu un zināmā mērā neitralizēšanu, šajā rokasgrāmatā aprakstītajā metodikā ieteikts iekļaut arī notikumu reģistrēšanu un, kas ir ļoti svarīgi, visos līmeņos iesaistīt procesus, ko piemēro, lai šo informāciju nodotu ieinteresētajām personām. Notikumu reģistrēšanai bieži vien nepievērš pietiekamu uzmanību, taču tai ir būtiska nozīme tiesu ekspertīzei un analīzei pēc notikuma.

Pilnīgā risinājumā jāiekļauj visa *C-UAS* vērtību ķēde, skat. 2. attēlu. Lai ieviestu daudzus risinājumus, sistēma vai sistēmas ir jāapvieno ar iesaistīto ieinteresēto personu procesiem vai procedūrām. Šī rokasgrāmata izstrādāta tā, lai lasītāji pakāpeniski izprastu katru aspektu, un tā iepazīstina ar pieciem posmiem, lai nonāktu līdz risinājumam. Katrā posmā ir izklāstīti ieteikumi un elementi, kas jāizpilda pirms attiecīgā posma, tā laikā un pēc tā.

Šajā iedaļā ir aplūkotas *C-UAS* risinājuma un *C-UAS* sistēmas atšķirības un iemesli, kāpēc jāievieš risinājums. Turpmāk 2. attēlā parādīta pilnīga šajā rokasgrāmatā izmantotā vērtību ķēde.

2. attēls. C-UAS risinājuma vērtību ķēde



Nākamajā iedaļā aprakstīti ieteiktie risinājuma ieviešanas posmi. Katra posma sākumā ir uzskaitīti elementi, kas nepieciešami, lai izpildītu attiecīgajam posmam paredzētos ieteikumus. Tie jāpapildina ar katram objektam atbilstīgu informāciju. Katras iedaļas beigās ir apkopots paveiktais un veicamās darbības pārejai uz nākamo posmu. Šos posmus ieteicams izpildīt secīgi. Ieteiktais risinājuma izstrādes process ir parādīts 3. attēlā.

3. attēls. Pieci C-UAS risinājuma izstrādes procesa posmi

Lasītājs varēs redzēt, kuri elementi ir jāizpilda un kuras ieinteresētās personas ir jāiesaista, lai izpildītu norādītās darbības. Šīs darbības vajadzēs izpildīt vēlāk – procesos vai posmos.

Protams, nevienu risinājumu nevar uzskatīt par statisku, un tam ir jāpilnveidojas, mainoties vajadzībām, objektiem, apdraudējumam un ieinteresētajām personām. Tā kā izmaiņas var būt gan īslaicīgas, gan pastāvīgas un var notikt jebkurā brīdī, risinājumi ir rūpīgi jāuzrauga un vajadzības gadījumā katra darbība ir jāatkārto. Izmantojot šo metodi, izmaiņas būs strukturētākas.

Turpmāk ir sniegts piecu posmu pārskats.

1. *C-UAS* sākuma posms. Šajā posmā ir aprakstītas pirmās ieteiktās darbības, kas jāveic, izpētot, vai ir nepieciešams *C-UAS* risinājums, un noteikti principi, mērķi un prasības attiecībā uz pārējo projekta daļu. Daudzos gadījumos iekšējās kompetences būs jāpapildina ar konsultācijām.

   - Darbības pamatojums un iespējamais sākums.
   - Pilnvaras, kas jāievēro.
   - Kur, kas un pret ko jāaizsargā.
   - Apzināt ieinteresētās personas un noteikt to funkcijas un pienākumus.
   - Apzināt juridisko pamatu, lai sāktu ieviešanu.
   - Informācijas vākšana par konkrētu objektu. Noteikt, kura iestāde atbild par izpildi, gaisa telpas pārvaldību, kartēm, plāniem, apdrošināšanu u. c.
   - Budžeta sadalījuma piešķiršana procesa sākšanai.

2. Riska un apdraudējuma analīzes posmā izpēta, analizē un dokumentē objekta *UAS* riskus un apdraudējumus, lai izstrādātu reaģēšanas plānu apdraudējuma gadījumiem. Šis plāns satur pamatinformāciju, ko izmantot pretpasākumu atlases procesā.

- Noteikt, pret ko ir jāaizsargā.
- Izprast riskus un izpētīt, kā tos iekļaut esošajos riska plānos.
- Definēt UAS riskus, izstrādājot scenārijus.
- Apzināt objekta kritiski svarīgos aktīvus, kuri ir neaizsargāti pret UAS.
- Objekta apsekojums.
- Reģionālie faktori. Vai notiek darbības KI tuvumā, pie robežām, vai attiecīgajā apgabalā tiek attīstīti UAS pakalpojumi?
- Pret kādiem makroriskiem KI mēģina aizsargāt?
- Riskam un risinājuma mērķim atbilstīga riska mazināšanas līmeņa izvēle.
- Reaģēšanas plāna izstrāde objekta apdraudējumiem.

3. Risinājuma izstrādes posmā reaģēšanas plānu apdraudējuma gadījumiem salāgo ar tehnoloģiju izmantošanu un ieinteresēto personu procesiem, lai efektīvi novērstu *UAS* radīto risku. Izstrādes procesā tiks iekļauta informācija par konkrēto objektu un tā vajadzības. Izstrādes process notiks, veicot izmēģinājumu un verifikācijas procesus. Tajā būs iekļauti risinājuma un tehnoloģijas izmēģinājuma plāni.

- Objekta specifiku salāgot ar vajadzībām, risku un apdraudējuma veidiem.
- Visām ieinteresētajām personām noteikt skaidras funkcijas un pienākumus.
- Noteikt, kā izmēģināt risinājumu un nodrošināt mācības ieinteresētajām personām.
- Pamatpakalpojumu minimuma īstenošana.
- Tādu tehnisko komponentu atlase, kuri spēs nodrošināt vajadzīgos riska mazināšanas pasākumus.
- Iestrādāt projektu arhitektūrā.

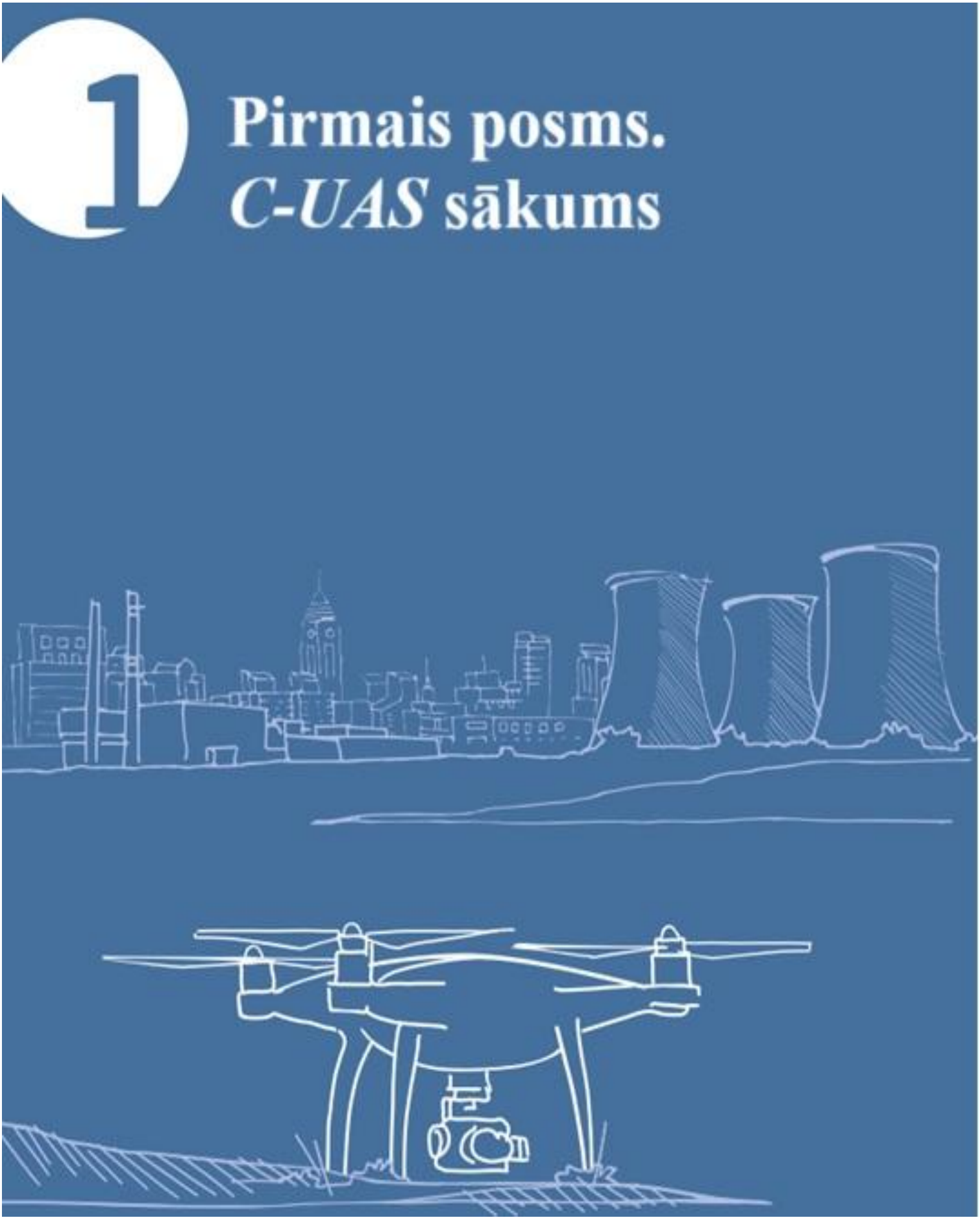
4. Risinājuma ieviešanas posmā ir sniegti norādījumi par to, kā ieviešamajā risinājumā tiks ņemti vērā dažādi apsvērumi saistībā ar ieviešanas procesu. Šajā posmā aprakstīts, kā izmantot izstrādāto projektu, un sniegti norādījumi par to, kas palīdzēs ieviest risinājumu sadarbībā ar ieinteresētajām personām.

- Risinājuma uzstādīšana.
- Ielaušanās testēšana.
- Iekārtu kalibrēšana un testēšana.
- Izstrādāt darbības plānus pēc ieviešanas un risinājuma pieņemšanas kritērijus.
- Pieņemšanas kritēriji un testēšana.
- Ekspluatācijas rokasgrāmatas un pāreja uz darbības režīmu.

5. Darbības posmā nosaka, kā ilgtermiņā uzturēt risinājuma darbību un saglabāt tā atbilstību objekta apdraudējuma veidiem. Darbības laikā risinājums būs jāuztur un jāatjaunina, un, ņemot vērā izmaiņas, piemēram, jaunus riskus, objekta pārmaiņas vai īpašus notikumus (piemēram, ļoti svarīgas personas (*VIP*) apmeklējumu), tas var tikt pilnveidots. Šā posma norise ir atkarīga no risinājumā paredzēto pretpasākumu konfigurācijas.

- Risinājuma darbība.
- Saziņa un ieinteresēto personu pastāvīga informēšana.
- Risinājuma pastāvīga atjaunināšana.

1 Pirmais posms. *C-UAS* sākums



Sākuma posms ir pirmais solis, ko veic, lai sāktu nodrošināt objektu pret nesadarbīgām *UAS*. Šajā posmā izpēta *C-UAS* risinājuma nepieciešamību un nosaka objekta principus, mērķus un sākotnējās prasības attiecībā uz *UAS* radītu apdraudējumu, riska analīzi, risinājuma atlases procesu un tā ieviešanu. Pirms *C-UAS* projekta uzsākšanas ir svarīgi saprast, ka situācijas apzināšanās, regulējuma jomas un procedūras var pastiprināt un atbalstīt pasīvos pretpasākumus (atturēšanu), objektam pašam neveicot lielus iepriekšējus ieguldījumus.

Nodoms aizsargāt pret *UAS* ir pats pirmais *C-UAS* risinājuma izstrādes posms, un tā mērķis ir mudināt sīkāk izpētīt *C-UAS* iespējas. Šo nodomu var ierosināt jebkurš notikums, piemēram, ap objektu konstatēta biežāka *UAS* pārvietošanās, dalībvalsts izlūkdienestu ieteikums, jaunu pastiprināta riska iekārtu uzstādīšana objektā vai tiesiskā regulējuma grozījumi. Šis nodoms sakņojas plašākā organizatoriskā kontekstā, un to ietekmē politiski, ekonomiski, sociāli, tehnoloģiski, vides vai juridiski faktori. Lai pamatotu jebkādas iniciatīvas, kas saistītas ar *C-UAS*, ir ļoti svarīgi skaidri noteikt darbības izraisītāju. Šādu izraisītājfaktoru piemēri varētu būt ar *UAS* saistīts incidents citā objektā vai jauns tiesību akts, kurā noteikta obligāta *C-UAS* risinājuma prasība.

1. IZCĒLUMS. PIRMAIS POSMS – SĀKUMS

Šajā posmā nepieciešamā informācija:

- izpratne par apdraudējumu (augsta līmeņa);
- izpratne par tiesību aktu prasībām;
- augsta līmeņa prasības;
- informācija par objektu un vidi.

Šā posma beigās jābūt izpildītiem turpmāk norādītajiem elementiem.

- Darbības pamatojums un skaidrs pilnvaru apraksts.
- Izpratne par to, kas pret ko un kur ir jāaizsargā.
- Tehnoloģiju izmantošanas ierobežojumi pretpasākumu risinājumā.
- Precizētas C-UAS risinājuma vajadzības, nosakot nepieciešamās darbības un projekta pārvaldību. Šeit jāiekļauj skaidra darbības joma, mērķi un sasniedzamie rezultāti.
- Informācija par objektu un vidi, kas varētu ietekmēt C-UAS risinājumu.
- Ieinteresēto pušu analīze (augstā līmenī).
- Izpratne par pamatpakalpojumu minimumu, kas nodrošinās sagatavošanos un ieviešanu.

Šajā pirmajā posmā ieteicams apkopot augsta līmeņa prasības attiecībā uz *C-UAS*, lai projekta gaitā tās precizētu sīkāk. Šādas prasības ietver:

- konkrētas objekta vajadzības un ierobežojumus, kas jāņem vērā projektā un risinājumā;
- informāciju par vidi;
- tehnoloģiju izmantošanu (piemēram, atļauju izmantot radiolokācijas tehnoloģiju, IKT sistēmas un datus, lai tie paliktu objektā īpašos serveros);
- izlūkošanu (piemēram, iestāžu informēšanu *C-UAS* incidenta gadījumā);

- tiesiskos un regulējuma ierobežojumus;
- jebkuras citas jomas, kas saistītas ar *C-UAS* risinājumu.

Šajā posmā svarīgi ir arī sākt ieinteresēto personu augsta līmeņa identificēšanu un sākt sarunas ar tiem.

DEFINĪCIJAS

***UAS* apkarošana** ir likumīga un droša bezpilota lidaparātu sistēmu radītu risku atklāšana, izsekošana, identificēšana un mazināšana.

***C-UAS* sistēma** ir *C-UAS* veikšanai izstrādātā risinājuma komponents.

***C-UAS* risinājums** ir *C-UAS* sistēmu un to ekspluatācijā iesaistīto ieinteresēto personu un procesu kopums.

1.1. DARBĪBAS PAMATOJUMS UN SKAIDRAS PILNVARAS

Lai sekmīgi īstenotu projektu, ir svarīgi, lai būtu skaidri definēts *C-UAS* risinājums un pilnvarojums sākt tā īstenošanu. Šo nodomu aizsargāt objektu vai infrastruktūru ir ļoti ieteicams dokumentēt, jo tā būs vieglāk iegūt lēmuma pieņēmēju un ieinteresēto personu atbalstu.

Projekta vadītājs un ieinteresētās personas darbības pamatojumu varēs izmantot kā norādi, un tajā būs iekļauts *C-UAS* mērķa apraksts, darbības joma, aplēstais termiņš un budžets, funkcijas un pienākumi, kā arī ieinteresēto personu informēšanai izmantotā pieeja.

Darbības pamatojumā ir jāizpilda turpmāk norādītie uzdevumi.

- Skaidri jānorāda pilnvarojums un pamatojums aizsardzības projekta sākšanai. Tas jānosaka augstākajam iespējamajam hierarhijas un institūciju līmenim.
- Jānosaka *C-UAS* risinājuma mērķis, darbības joma un rezultāts.
- Jānosaka objektam nepieciešamais riska mazināšanas līmenis (piemēram, vai mērķis ir uzraudzība, pasīva iejaukšanās vai aktīva iejaukšanās).
- Jādokumentē risinājuma pielīdzināšana atbilstīgi objekta drošības vajadzībām.
- Jādokumentē īstermiņa un ilgtermiņa stratēģiskie mērķi.
- Jāpamato ieguldījums un jānosaka budžeta sadalījums.
- Jāapraksta *C-UAS* risinājuma juridiskais pamats.
- Jādefinē pirmās ieinteresētās personas, kuras jāiesaista, un jānosaka to funkcijas un pienākumi.

Šāda darbības pamatojuma formātu var izstrādāt atbilstīgi paša objekta projekta vadības metodikai.

1.2. DOMĀT PAR RISINĀJUMU, NEVIS SISTĒMU

Jau pašā procesa sākumā ir svarīgi gūt skaidru priekšstatu par to, kas ir nepieciešams, lai mazinātu visus apzinātos riskus. Ļoti svarīgi ir izprast atšķirību starp *C-UAS* sistēmu un risinājumu. *C-UAS* sistēmas parasti veido vairāki savstarpēji apvienoti un sasaistīti tehniski komponenti. Parasti tie ir atklāšanas, izsekošanas un identificēšanas komponenti, kāds operatora veids, kas palīdz klasificēt *UAS* un apdraudējuma veidus, daži paredzēti sistēmas reģistrēšanai un dažos gadījumos neitralizācijai, skat. 2. attēlu.

Lai gan daudzos gadījumos tas var palīdzēt mazināt risku, *C-UAS* ieteicams veidot kā vienotu risinājumu. Risinājums var ietvert vairākas sistēmas un papildu pakalpojumus un procesus. Lai arī tas sarežģīs ieviešanu, tas noteikti palīdzēs uzlabot aizsardzību. Pienācīgi ieviestu risinājumu būs arī vieglāk pilnveidot atbilstīgi (īslaicīgām vai pastāvīgām) apdraudējuma vides izmaiņām.

Papildus *C-UAS* sistēmas elementiem *C-UAS* risinājumā (skat. 2. attēlu) ir ņemti vērā darbības un ieinteresēto personu procesi, organizatoriskie un ārējie faktori, piemēram, reģionālie noteikumi. Risinājumā var būt arī iekļauta neitralizācija un notikumu tiesu ekspertīzei un turpmākiem uzlabojumiem nepieciešamās informācijas reģistrēšana.

Risinājums ir jāiekļauj esošajos ieinteresēto personu procesos, un tam jānodrošina informācijas apmaiņa ieinteresēto personu starpā.

2. attēlā parādīta *C-UAS* risinājuma vērtību ķēde, un turpmākajā sarakstā ir aprakstīti vairāki svarīgi elementi, kas ir iekļauti visos risinājumos.

- Atklāšanas tehnoloģijas, izsekošanas un identificēšanas sistēmas. Tās var būt no dažādiem piegādātājiem un var apvienot izvaddatus, izmantojot sensoru apvienošanu.
- Asistēts lēmumu pieņemšanas process un automatizēti procesi, izmantojot savstarpēji savienotas sistēmas. Tas palīdzēs operatoriem optimāli izmantot risinājumu.
- Datu reģistrācija, kas ietver gan notikumus no sistēmām, gan no ieinteresēto personu procesiem. Visi notikumi ir jāapvieno un tajos jāiekļauj novērojumi, notikumi, par kuriem ziņots, izmantojot citus kanālus (pa tālruni vai manuāli), *U-Space*[5] un bezpilota lidaparātu sistēmu satiksmes vadības (*UTM*) notikumi, citas ģeogrāfiskās zonas un blakus esošie objekti, sabiedriskie pakalpojumi, tiesībaizsardzības iestādes (*LEA*) utt.
- Risinājumā ir jāiekļauj daudzi ieinteresēto personu procesi, un tas ir pastāvīgi jāvērtē. Procesos jāiekļauj turpmāk minētie elementi.
-
  - Iestāžu informēšana par incidentu.
  - Mijiedarbība un vienošanās ar tiesībaizsardzības iestādēm. Tā būs iespējams zināt, kas un ar ko sazināsies incidenta gadījumā, kurš ko un kad darīs.
  - Vienošanās ar gaisa telpas pakalpojuma sniedzējiem (*UTM*, *U-Space*).
  - Mijiedarbība ar iestādēm un blakus esošiem objektiem.
  - Datorizēta nosūtīšana.
  - Neitralizēšanas atļaujas pieprasījums ieinteresētajai personai, kura ir pilnvarota pieņemt šādu lēmumu.
  - Tiesu ekspertīzes datu apmaiņa.
  - Saziņa ar ieinteresētajām personām, kuras skar vai ietekmē risinājums.

[5] https://www.sesarju.eu/U-space

1.3. SADARBSPĒJA UN IZSTRĀDES PRINCIPI

Ikviens *C-UAS* risinājums ir sadarbspējas īstenošana juridiskā, organizatoriskā, semantiskā un tehniskā līmenī. Ieinteresētajām personām ieteicams izmantot šajā iedaļā aprakstītos risinājuma izstrādes principus un katru rokasgrāmatā iekļauto posmu pārbaudīt, salīdzinot ar Eiropas sadarbspējas sistēmu[6], skat. 4. attēlu.

4. attēls. Eiropas sadarbspējas sistēma

Avots. Eiropas sadarbspējas sistēma (pielāgota).

- **Juridiskā sadarbspēja** ļauj organizācijām darboties, ievērojot atšķirīgus valstu tiesiskos regulējumus, politikas nostādnes un stratēģijas, lai strādātu kopā. Valstu tiesību akti un politikas nostādnes var liegt sadarbību, tāpēc ieinteresēto personu grupām ir skaidri jāvienojas, kā rīkoties atšķirīgu tiesību normu gadījumos.

- **Organizatoriskā sadarbspēja** ir veids, kā valsts pārvaldes iestādes (t. i., valdības iestādes un organizācijas) saskaņo savus darba procesus, pienākumus un gaidāmos rezultātus, lai sasniegtu kopīgi saskaņotos mērķus. Praksē organizatorisko sadarbspēju īsteno kā darba procesu dokumentēšanu, integrēšanu vai pielāgošanu un attiecīgās informācijas apmaiņu.

- **Semantiskā sadarbspēja** nodrošina, ka pēc datu apmaiņas ir saglabāts un saprasts precīzs datu un informācijas formāts un jēga: "nosūtītais ir saprasts". Tas ietver tādus sintakses aspektus kā terminoloģija, ko izmanto, lai aprakstītu koncepcijas un precīzu informācijas formātu.

- **Tehniskā sadarbspēja** attiecas uz lietojumu un infrastruktūru sistēmu un pakalpojumu sasaisti. Tostarp ir tādi aspekti kā saskarnes un pakalpojumu specifikācijas, datu un metadatu standarti un formāti.

[6] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail.

Ieviešot risinājumu, ieteicams visos posmos atcerēties šos principus.

Līdztekus sadarbspējai visiem risinājumiem jābūt:

- **atbilstīgiem** – pēc ieviešanas risinājumam jāatbilst KI vai sabiedrisko vietu vajadzībām un jāmazina apzinātais risks;
- **efektīviem** – risinājumam jāmazina riski un incidenti, kad tie notiek;
- **lietderīgiem** – lai praktiski mazinātu riskus un incidentus (lai to panāktu, risinājumam jābūt pienācīgi ieviestam un jādarbojas pareizi);
- **saskaņotam** – saskaņoti risinājumi ir pielīdzināti pasākumiem, ko veic līdzīgās KI vai sabiedriskajās vietās, un tuvējā apkārtnē ieviestajiem pasākumiem;
- **iedarbīgam** – risinājumu iedarbībai jābūt izmērāmai, ņemot vērā to, kā tie mazina vai ierobežo incidentu sekas;
- **ilgtspējīgam** – ilgtspējīgi risinājumi pilnveidosies, mainoties videi, apdraudējuma veidiem un KI.

Izmantojot projekta vadības metodiku[7], projekta vadītāji varēs sniegt risinājumus un ieguvumus savām organizācijām, efektīvi pārvaldot visu savu projektu darbības ciklu. Tā būs vieglāk standartizēt, strukturēt un grupēt vajadzības un risinājuma ieviešanu.

Izstrādājot risinājumu, ļoti ieteicams izmantot atvērtos saziņas standartus un protokolus. Piegādātājam varētu būt savs protokols, ko izmanto un kas sekmīgi darbojas, taču, pievienojoties citām sistēmām un integrējot sistēmas lielākā risinājumā, tas bieži kļūst apgrūtinošs un sarežģīts, un tādēļ vajadzīgi papildu resursi un laiks.

1.4. KAS, PRET KO UN KUR IR JĀAIZSARGĀ?

Risinājuma izstrādes procesa sākumā svarīgs posms ir *C-UAS* risinājuma pirmo augsta līmeņa vajadzību noteikšana un aprakstīšana. Šajā posmā, iespējams, vēl nav pilnīgi skaidras izpratnes, definīcijas vai apraksta par to, kas un pret ko ir jāaizsargā. Pirms risinājuma izstrādes uzsākšanas un tehnoloģiju sistēmu izvēles ir ļoti svarīgi formulēt šīs definīcijas. Daudzos gadījumos var būt ļoti grūti iegūt skaidru atbildi, un, lai precizētu pieeju, ir nepieciešami riska novērtējumi. Sākot pētīt aizsardzību pret *UAS*, ir svarīgi jau sākumā zināt, kas ir jāaizsargā, kāda ir juridiskā forma, KI darbības vajadzības, integrācijas līmenis gaisa telpas pārvaldībā, valsts un reģiona robežas, kas un ko drīkst darīt, kā arī apsvērumi par ieinteresēto personu iekļaušanu.

Jo labāk ir izstrādāts apraksts, jo vieglāk būs pieņemt lēmumus vēlākā procesa gaitā. Visi parametri ir ļoti lielā mērā saistīti un ir jāreģistrē, tādējādi iegūstot augsta līmeņa aprakstu, kas nepieciešams nākamajiem riska novērtēšanas un risinājuma izstrādes posmiem.

[7] Sk. *PM²* projekta vadības metodiku.

Kas pret ko ir jāaizsargā?

Pretpasākumu efektivitāte ir atkarīga no mērķa veida (piemēram, cilvēki, *VIP*, dati, infrastruktūra), tā neaizsargātības un noziedzīgā nodarījuma izdarītāja nodoma. Šajā posmā ir svarīgi arī dokumentēt *UAS* veidus, ko varētu izmantot uzbrukumā.

5. attēls. Galvenie kritiskās infrastruktūras UAS apdraudējuma veidi

Turpmāk uzskaitītas iespējamās apdraudējuma kategorijas, kas pēdējos gados apzinātas civilajā kontekstā.

- **Bīstamu kravu nosūtīšana.** *UAS* kravnesība pēdējos gados ir palielinājusies, pateicoties efektīvākiem motoriem un baterijām, tāpēc tās var izmantot improvizētu sprāgstierīču, granātu vai ķīmisko, bioloģisko, radioloģisko vielu un kodolvielu nosūtīšanai drošā perimetrā. Uzlabotā precizitāte, ko nodrošina videokameru un ierīču izmantošana, ļauj modernajām *UAS* lielos attālumos pārvadāt lielas kravas. Kravas var novietot izvēlētā vietā, piemēram, uz ēkas jumta, un var nomest, izmantojot īpaši konstruētu mehānismu, vai aktivizēt gaisā, vai pat apzināti pilotēt pret neaizsargātu objektu, veicot "kamikadzes" tipa uzbrukumu. Iespējamie mērķi ir konkrētas personas, KI, sabiedriskas vietas, informācijas tehnoloģiju sistēmas un pakalpojumi (piemēram, enerģijas ražošanas uzņēmumi, finanšu iestādes, valsts pārvaldes iestādes, aizsardzības infrastruktūra).

- **Kontrabanda/piegāde.** Eiropā jau ir novēroti vairāki gadījumi, kad *UAS* ir izmantotas aprīkojuma piegādei uz izvēlētām vietām, jo tās spēj viegli šķērsot ierastos kontroles punktus un iekļūt aizsargātās vietās. Piegādāto aprīkojumu (piemēram, šaujamieročus) var izmantot agresors, kas drošajā zonā jau ir iekļuvis, izmantojot parasto kontroles procedūru. Piemēram, ļoti daudzas dažādas kravas (piemēram, mobilie tālruņi, narkotiskās vielas, nelegālas preces, ieroči), jau ir piegādātas cietumos vai nelegāli pārvestas pār starptautiskajām robežām.

- **Propaganda.** *UAS* var izmantot arī protestētāji un teroristu grupas, lai ierakstītu savas darbības, sabiedriskās vietās izplatītu brošūras vai citus materiālus savos centienos pastiprināt propagandu. Uzfilmēto materiālu var pārraidīt tiešsaistē, lai piesaistītu piekritējus un mudinātu savervēt jaunus teroristus vai protestētājus, jo tas rada iespaidu, ka organizācija ir sekmīga un tajā strādā mērķtiecīgi dalībnieki.

- **Iejaukšanās un traucēšana.** Pat *UAS* klātbūtne vien var būt pietiekama, lai traucētu aktīva normālo darbību, jo tā rada drošuma problēmas (piemēram, civilās aviācijas traucējumi, lidojumi virs publikas koncerta laikā). Traucējumus var radīt arī dažādos masu pasākumos pilsētas teritorijā, izraisot klātesošās publikas panikas reakciju, kuras dēļ cilvēki var gūt traumas, iet bojā, vai radīt labvēlīgus apstākļus sekundāram uzbrukumam (piemēram, novirzīt cilvēkus uz konkrētām vietām).

- **Izlūkošana, uzraudzība un rekognoscēšana.** *UAS* var izmantot arī, lai vāktu informāciju un novērotu darbības, galvenokārt izmantojot videokameras, kā arī videokameras ar nakts redzamību vai termiskajiem sensoriem. Tā noziedzīga nodarījuma izdarītāji no droša attāluma var iegūt informāciju par potenciālā mērķa neaizsargātību un to izmantot uzbrukumā vai pat uzbrukuma gaitā sniegt informāciju reāllaikā. Pēdējā laikā ir izstrādāti arī jaudīgi mikrofoni, kas ļauj slepus noklausīties privātas/konfidenciālas sarunas. Turklāt privātus attēlus, ko uzņēmušas *UAS*, pārkāpjot indivīdu privātumu, var izmantot noziedzīgiem nolūkiem, piemēram, krāpšanai vai šantāžai.

- **Traucējumu radīšana.** *UAS*, kurās uzstādītas attiecīgas elektroniskās iekārtas, var izmantot lokālu traucējumu radīšanai, lai traucētu perimetra drošības sistēmu, *GPS* sistēmu vai mobilo tālruņu signālu darbību. Šis taktiskais paņēmiens var radīt papildu neaizsargātību, ko var izmantot noziedzīga nodarījuma izdarītājs vai kas var būtiski ietekmēt aktīva (piemēram, lidostas) darbības.

- **Kiberuzbrukumi.** *UAS* var apdraudēt kiberdrošību, uzbrūkot vietējiem bezvadu tīkliem un traucējot sakarus, piegādājot ļaunatūras, nolaupot un/vai manipulējot sensitīvus datus. To var izdarīt ar īpašām iekārtām, kas piekļūst bezvadu sistēmai. Turklāt *UAS* var kļūt par kiberuzbrukuma mērķi (zināma arī kā "*UAS* uzlaušana"), jo noziedzīga nodarījuma izdarītāji var iegūt kontroli pār to un mainīt tās maršrutu, iegūt piekļuvi tās datiem vai to iznīcināt (piemēram, pakalpojuma atteikums).

Tā kā pieaug *UAS* komerciālās, profesionālās un izklaides izmantošanas iespējas un daudzas ar *UAS* izmantošanu saistītās tehnoloģijas vēl tikai attīstās, ir skaidrs, ka 5. attēlā apkopoto apdraudējumu kategorijas paplašināsies. Labāki akumulatori un dzinēji nodrošinās ilgāku lidojuma laiku ar lielāku derīgo kravu, toties ātrdarbīgāki mobilie tīkli (5G) nodrošinās iespēju sazināties lielos attālumos, bet mākslīgā intelekta lietotnes var izmantot, lai uzlabotu *UAS* sadarbību, veidojot to grupas.

Pret ko ir jāaizsargā?

Parasti incidentu izraisītājus iedala šādās kategorijās: atbilstīgi/rūpīgi, nezinoši, nevērīgi lietotāji un noziedznieki/teroristi. Incidenta brīdī var nebūt iespējams noteikt, kurai grupai izraisītājs pieder, un klasifikācija varbūt būs iespējama tikai pēc notikušā incidenta analīzes. Neatkarīgi no iemesla, atklājot *UAS* vietā, kurā tam nebūtu jāatrodas, pret to ir jāveic pienācīgi pretpasākumi. Pašreizējo klasifikāciju var izmantot, lai atjauninātu priekšstatu par apdraudējumu un varētu veikt risinājuma turpmākos atjauninājumus un to pilnveidot.

Atbilstīgo, nezinošo, nevērīgo un noziedzīgo grupu klasifikāciju, skat. 6. attēlu, var izmantot apdraudējuma novērtēšanā, lai klasificētu pilota nodomu vai motivāciju.

- **Atbilstīgi/rūpīgi** piloti ievēro noteikumus un tiesisko regulējumu, taču tehnisku vai ar darbību saistītu apstākļu dēļ bezpilota lidaparāts var iekļūt neatļautā zonā un kļūt par neatļautu bezpilota lidaparātu (piemēram, vadības zuduma, vēja vai tehnisku traucējumu dēļ).

- **Nezinošas** personas, kas nezina vai neizprot piemērojamos noteikumus un ierobežojumus. Tāpēc tie darbojas ierobežotas piekļuves zonā. Parasti tie nevēlas nodarīt kaitējumu.

- **Nevērīgas** personas zina piemērojamos noteikumus un ierobežojumus, taču kļūmes vai nolaidības dēļ tos pārkāpj. Tāpēc tie savus bezpilota lidaparātus pilotē ierobežotas piekļuves zonās.

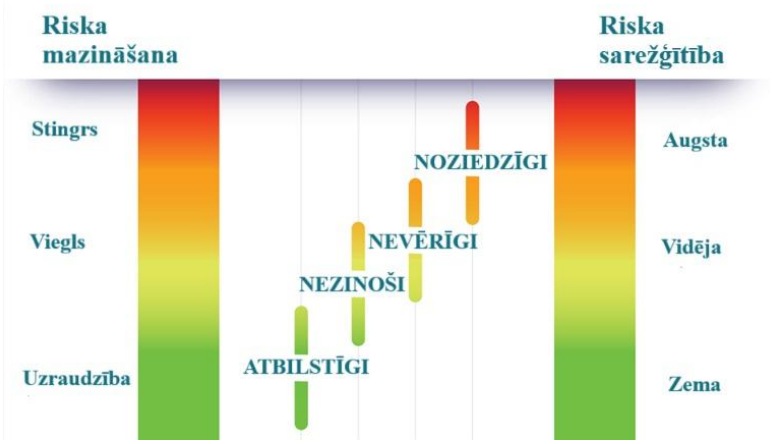
- **Noziedznieki/teroristi** ir personas, kuras neatkarīgi no tā, vai pārzina piemērojamos noteikumus un ierobežojumus, aktīvi cenšas ļaunprātīgi izmantot *UAS*, lai pārkāptu drošumu un drošību KI ierobežotas piekļuves zonās vai sabiedriskās vietās.

6. attēls. *UAS* lidojumu kategorijas

Nepieciešamie risinājumi noteikti būs pilnīgi atšķirīgi atkarībā no tā, kas un pret ko tiek aizsargāts. Var pieņemt, ka noziedznieki veiks sarežģītus un plānotus uzbrukumus. Viņi var izmantot pārveidotas *UAS* un, piemēram, izmantot pārveidotus *UAS* sakaru signālus, lai varētu izvairīties no atklāšanas vai identifikācijas.

Nodrošinot aizsardzību pret noziedzniekiem, risinājumā bieži vien būs vajadzīgi "stingri" riska mazināšanas pasākumi, tāpēc šis ir viens no vissarežģītākajiem un problemātiskākajiem apdraudējumiem, pret ko aizsargāt, skat. 7. attēlu.

7. attēls. Dažādu UAS lietotāju kategoriju riska mazināšana un pretpasākumu sarežģītība



Bieži ir jānošķir sadarbīgas un nesadarbīgas *UAS*.

- **Sadarbīgu *UAS*** piloti izpildīs tiesiskās prasības, un viņiem būs nepieciešamās atļaujas lidojumiem gaisa telpā. Tās ir iepriekš minētās atbilstīgās personas. Tomēr ārēju faktoru dēļ šāds lidojums var kļūt par apdraudējumu, kas jānovērš.

- **Nesadarbīgu *UAS*** piloti ir gan nezinoši, gan nevērīgi un noziedzīgi lietotāji. Šie lietotāji pilotēs *UAS*, kur vien vēlēsies, un viņiem var būt vai nu ļaunprātīgi nodomi, vai arī viņi var kļūt par apdraudējumu nejaušības vai darbības traucējumu dēļ.

Neatkarīgi no izmantotās klasifikācijas ir ļoti svarīgi atcerēties, ka nekad nebūs iespējams noteikt faktisko kategoriju.

Kur aizsargāt?

Pieņemot lēmumu par to, ko aizsargāt, vēlams klasificēt objektā esošos elementus. Vai kādas daļas ir svarīgākas un ir jāaizsargā vairāk? Kur atrodas vissvarīgākie elementi? Vai tie atrodas tālu no objekta robežām vai to tuvumā vai pie robežām, kas varētu būt svarīgas? Tādi vides faktori kā lauku vai pilsētas apkārtne ir jādokumentē.

PADOMS

Ja bezpilota lidaparāts, pārkāpjot noteikumus un tiesību aktus, atrodas gaisa telpā, kurā tam nevajadzētu būt, tas varētu radīt risku, un šis risks ir jāmazina, piemērojot pieņemtos pasākumus.

1.5. IEINTERESĒTO PERSONU VADĪBA

C-UAS risinājuma ieviešanas procesa sākuma posmos ir jāiesaista ieinteresētās personas. Tiklīdz ir apstiprinātas vienošanās ar iekšējām saimnieciskajām vienībām un ir pieņemts lēmums sākt risinājuma izstrādi, ir jāsāk iekšējo un ārējo ieinteresēto personu piesaiste. Iepriekš 2. attēlā bija redzams, ka ieinteresēto personu iesaistīšanas process ir ļoti svarīgs un ir savstarpēji saistīts ar visām sistēmām. Jebkurā projekta vadības metodikā būs iekļauti daži ieinteresēto personu iesaistes elementi. Ieinteresēto personu apzināšana un analīze var būt laikietilpīgs un visaptverošs process. Tas regulāri jāpārskata, lai nodrošinātu tā atjaunināšanu un pilnīgumu. Jāsāk ar zināmām ieinteresētajām personām un jāizmanto tās.

Ieinteresēto personu iesaistei *C-UAS* risinājuma izstrādē ir būtiska nozīme. Daži no ieguvumiem izklāstīti turpmāk.

- **Projekta panākumu nodrošināšana.** Ieinteresētās personas var sniegt vērtīgu ieguldījumu visā projekta darbības ciklā – sākot no sākotnējiem plānošanas posmiem līdz pat ieviešanai un izvērtēšanai. To iesaistīšana nodrošina projekta pielīdzināšanu gaidāmajiem rezultātiem, vajadzībām un mērķiem, kas palielina panākumu iespējamību.

- **Risku apzināšana.** Ieinteresētās personas var apzināt iespējamos riskus, kas var ietekmēt projekta panākumus. Tā projekta vadītāji var mazināt šos riskus vai no tiem izvairīties, pirms tie kļūst par būtiskām problēmām.
- **Atbalsta saņemšana.** Iesaistot projektā ieinteresētās personas, varēsit saņemt to atbalstu un piekrišanu, tādējādi palīdzot pārvarēt pretestību pret pārmaiņām vai iespējamos šķēršļus, kas varētu rasties projektā.
- **Gaidāmo rezultātu pārvaldība.** Ieinteresēto personu iesaiste var palīdzēt pārvaldīt to gaidāmos rezultātus un novērst pārpratumus. Tas palīdzēs nodrošināt, ka ikviens iesaistītais skaidri saprot, ko no viņa sagaida un kādus projekta mērķus paredzēts sasniegt.
- **Saziņas uzlabošana.** Ieinteresēto personu iesaiste palīdzēs noteikt skaidrus saziņas virzienus starp projekta vadītājiem, ieinteresētajām personām un grupas locekļiem. Tas veicinās pārredzamību, mazinās konfliktu rašanos un uzlabos izpratni par projekta virzību un rezultātiem.

Tā kā iesaistītās ieinteresētās personas ir dažādas, ir ieteicams un ir svarīgi pirmo ieinteresēto personu karti izstrādāt pēc iespējas agrāk.

Kartēšanā jānorāda vismaz tie dalībnieki, kurus skar risinājums, un tie, kas iesaistīti risinājuma darbībā vai informācijas apmaiņā par to. Sākumā šīs ārējās ieinteresētās personas var būt tikai no brīdinājuma zonas un *UAS* ģeogrāfiskās zonas perimetra.

Tā kā *UAS* risinājumi blakus esošos objektos un apkārtnē būs svarīgs informācijas avots un ir jāizvairās no tehnoloģiju pārklāšanās, arī no šīm vietām ir jāiekļauj ieinteresētās personas.

Notikumu uzraudzībai un neitralizācijai svarīgas ieinteresētās personas ir *LEA* (vietējais, reģionālais un federālais līmenis). Dažādu *LEA* līmeņu pienākumi atšķirsies, tāpēc ir svarīgi kartēt pienākumus.

Turpmāk ir uzskaitītas galvenās ieinteresētās personas, ar kurām jāapspriežas jebkurā projektā:

- risinājuma tiešie lietotāji;
- līdzīgi KI objekti;
- iestādes un regulatīvās iestādes, kas atbild par aizsargājamo objektu;
- iestādes, kam uzticēta riska un apdraudējuma novērtēšana;
- pārvaldes iestādes, kas atbild par infrastruktūru un risinājuma atrašanās vietu;
- aizsargājamā objekta vadība;
- drošuma un drošības dienesti;
- iestādes, kas regulē aizsargājamo objektu;
- *LEA* (vietējais, reģionālais un federālais līmenis);
- iestādes, kas iesaistītas risku mazināšanā (un kurām ir atļauja to darīt);
- izlūkošanas un drošības iestādes;
- gaisa telpas pārvaldnieki un *UTM*/*U-Space* ieinteresētās personas aizsargājamā objekta tuvumā;
- aizsargājamam objektam blakus esoši objekti;

- regulējuma iestādes, kas atļauj izmantot tehnoloģijas (piemēram, radiolokatoru frekvences un iespējamā bloķēšana);
- sistēmas integratori.

Katram ieviešamajam risinājumam var būt atšķirīgas ieinteresētās personas. Daudzas ieinteresētās personas un dalībniekus savstarpēji saista kopīga izpratne par apdraudējumu un saistītajiem riskiem. Tāpēc visos risinājuma izstrādes un ieviešanas posmos ir svarīga laba ieinteresēto personu vadība.

Turpmāk 8. attēlā ir sniegts *RASCI* (atbildīgs, pārskatatbildīgs, atbalstošs, iesaistīts apspriešanā, informēts) tabulas[8] piemērs, ko var izmantot, lai kartētu ieinteresēto personu iesaisti. Šāda tabula ir jāpapildina, iekļaujot konkrētas apzinātās un ar aizsargājamo objektu saistītās ieinteresētās personas. Šis posms atbilst *C-UAS* izstrādes procesa ceļvedim, kā parādīts 14. attēlā.

PADOMS

Jāapzinās, ka katrā risinājumā var būt atšķirīgas iesaistītās ieinteresētās personas. Jo spēcīgāka aizsardzība, jo sarežģītāka ir ieinteresēto personu vadība.

Izstrādes posmā ieinteresēto personu iesaiste tiks izstrādāta sīkāk.

8. attēls. C-UAS risinājuma izstrādes procesā iesaistīto ieinteresēto personu RASCI matricas piemērs (jāpapildina atbilstīgi konkrētām vajadzībām)

Ieinteresēto personu kategorija	Ieinteresētās personas	Pirmais posms *C-UAS* sākums	Otrais posms *UAS* riska novērtēšana, lai papildinātu esošo riska novērtējumu	Trešais posms *C-UAS* risinājuma izstrāde	Ceturtais posms Risinājuma ieviešana	Piektais posms Risinājuma ieviešana
Objekts	KI saimnieciskās darbības īpašnieks	A	A	A	A	A
	Vietējie drošības dienesti	R	R	R	R	R
	Vietējā kopiena un blakus esoši objekti	I	I, C	I, C	I	I
	Līdzīgi KI objekti	C	S	C	S	
	Organizācijas regulators	S	C	C	I	S
Iestādes	Tiesībaizsardzība	C	C	I	I	S

[8] Sk. *PM²* projekta vadības metodiku.

	Iestādes, kurām ir atļauts izmantot riska mazināšanas pasākumus	C	C	C	R	R
	Iestādes, kas regulē tehnoloģiju izmantošanu	C	I	C	I	I
Valsts pārvaldes struktūras	Iestādes, kam uzticēta riska un apdraudējuma novērtēšana	C	C	I	I	C
	Pārvaldes iestādes	C	C	S	C	I
Privātas struktūras	Telesakaru operatori	C	C		S	
	C-UAS risinājuma piegādātāji	S	C	C	C	C
Gaisa telpa	*UTM* pakalpojumi	C	C	C	R	R
	U-space pakalpojuma sniedzējs	C	I, C	I	C	I

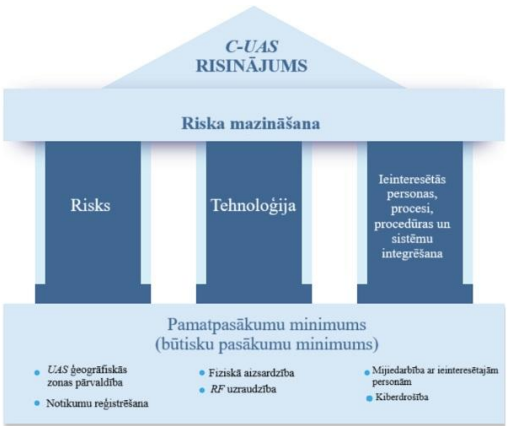
R = atbildīgs	A = pārskatatbildīgs	S = atbalstošs	C = iesaistīts apspriešanā	I = informēts

1.6. PAMATPASĀKUMU MINIMUMS

Pamatpasākumiem ir būtiska nozīme, un tie ir kopīgi visiem risinājumiem, tāpēc tie ir jāpārdomā un jāiekļauj vairākumā risinājumu. Šo pasākumu īstenošana ļaus risinājumam attīstīties atbilstīgi riska līmeņa izmaiņām, atjauninot vai mainot tehnoloģijas, mainoties procesiem, un sagatavos datu apmaiņai ar ieinteresētajām personām.

Tie ir pakalpojumi, kas vienmēr ir vajadzīgi un kas jāīsteno jau agrīnā posmā. Sīkāku informāciju par šo pakalpojumu izstrādi skat. 3.1. iedaļā.

9. attēls. Pamatpasākumu minimums, kas atbalsta citus C-UAS risinājuma pīlārus



Pamatpasākumu minimumā iekļauti turpmāk minētie pasākumi.

- ***UAS* ģeogrāfiskās zonas pārvaldība** ir gaisa telpas pārvaldība, ko izveidojusi kompetentā iestāde *UAS* operāciju atvieglošanai, ierobežošanai vai aizliegšanai, lai novērstu riskus, kas saistīti ar drošumu, privātumu, personas datu aizsardzību, drošību vai vidi un kas izriet no *UAS* operācijām[9]. Tā ietver atļauju ekspluatēt *UAS*, izmantot *C-UAS* tehnoloģijas un izmēģināt *UAS* risinājumu. Savlaicīgi ir jāsāk pētīt gaisa telpas pārvaldības rīku izmantošanas iespējas, piemēram, *UTM* izmantošana un saites uz *U-Space* pakalpojumiem, jo šos rīkus ir svarīgi integrēt citos risinājumos, kas ieviesti ap aizsargājamo objektu. Tā ietver arī ieinteresēto personu vadību objekta apkārtējās zonās.

- **Notikumu reģistrēšanu** veic, lai izprastu, kas notiek jūsu gaisa telpā, reģistrējot visas *UAS* izmantošanas darbības un novērojumus aizsargājamā objektā un tā apkārtnē. Reģistrēšanai jāaptver visi datu avoti un novērošanas pasākumi. Reģistrācija jāveic cik vien iespējams pilnīgi, lai to varētu izmantot turpmākai risku analīzei un iespējamai tiesu ekspertīzei.

- **Fiziskā aizsardzība** ir svarīgs elements, ar ko jāsāk agrīnos posmos, apsverot riskus ēkām un fiziskajai infrastruktūrai, kā arī konstrukciju iespējamo modernizāciju vai izmaiņas. Šīs iniciatīvas veic, ņemot vērā *UAS* veidus, pret kuriem jāveic pretpasākumi. Nākamajos posmos, kad ir precizēti riski, tā ir jāpārvērtē. Sīkāku informāciju skat. *JRC* rokasgrāmatā par fizisku aizsardzību pret *UAS*[10].

- ***RF* uzraudzība** attiecībā uz *UAS* ir atklāšanas minimums, ar ko jāsāk visām aizsargātām gaisa telpām. Lai gan tās mērķis ir atklāt iespējami vairāk *UAS*, ir skaidrs, ka tās visas nav iespējams atklāt. Ar šo metodi atklāj un nolasa *UAS*, raidītos signālus un sakarus starp *UAS* un tās bāzes staciju. Attālā ID, ko raida *UAS*, ietver svarīgus parametrus, ko var izmantot gaisa telpas pārvaldībai. Interpretējot saziņu starp zemes staciju/pilotu un *UAS*, var iegūt papildu informāciju. Šie avoti papildina cits citu un kopā ar atrašanās vietas noteikšanu nodrošina ļoti labu pamata pārskatu par gaisa telpu. Jānorāda, ka šādi nevarēs atklāt tumšās *UAS*[11], kas programmētas, lai lidotu, nesazinoties ar vadības bāzes staciju. Tā nevarēs atklāt arī *UAS*, kas pārveidotas, lai neraidītu šos signālus vai izmantotu nestandarta frekvences. Lai nodrošinātu maksimālu aptvērumu, ieteicams novērot frekvences un diapazonus ap tādiem, ko parasti izmanto *UAS*, un izvairīties no specifiskām izplatītāju sistēmām, kas nosaka tikai savas *UAS*.

- **Mijiedarbība ar ieinteresētajām personām** ir viens no svarīgākajiem risinājuma procesiem, pret ko bieži vien izturas nevērīgi un ko nenovērtē. Visas sistēmas var uzstādīt un darboties atbilstīgi specifikācijām, bet bez ieinteresēto personu iesaistīšanās un integrācijas, kas vajadzīga, lai pieejamajā laikposmā mazinātu apdraudējumu, šīs sistēmas var būt nelietderīgas. Kā redzams 2. attēlā, ieinteresēto personu iesaistīšanas process attiecas uz visām sistēmām un visiem vērtību ķēdes elementiem.

[9] Komisijas Īstenošanas regula (2019. gada 24. maijs) (ES) 2019/947 par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32019R0947.

[10] Aizsardzība pret bezpilota lidaparātu sistēmām. Rokasgrāmata par bezpilota lidaparātu sistēmu riska novērtēšanu un ēku un objektu fizisku nostiprināšanu

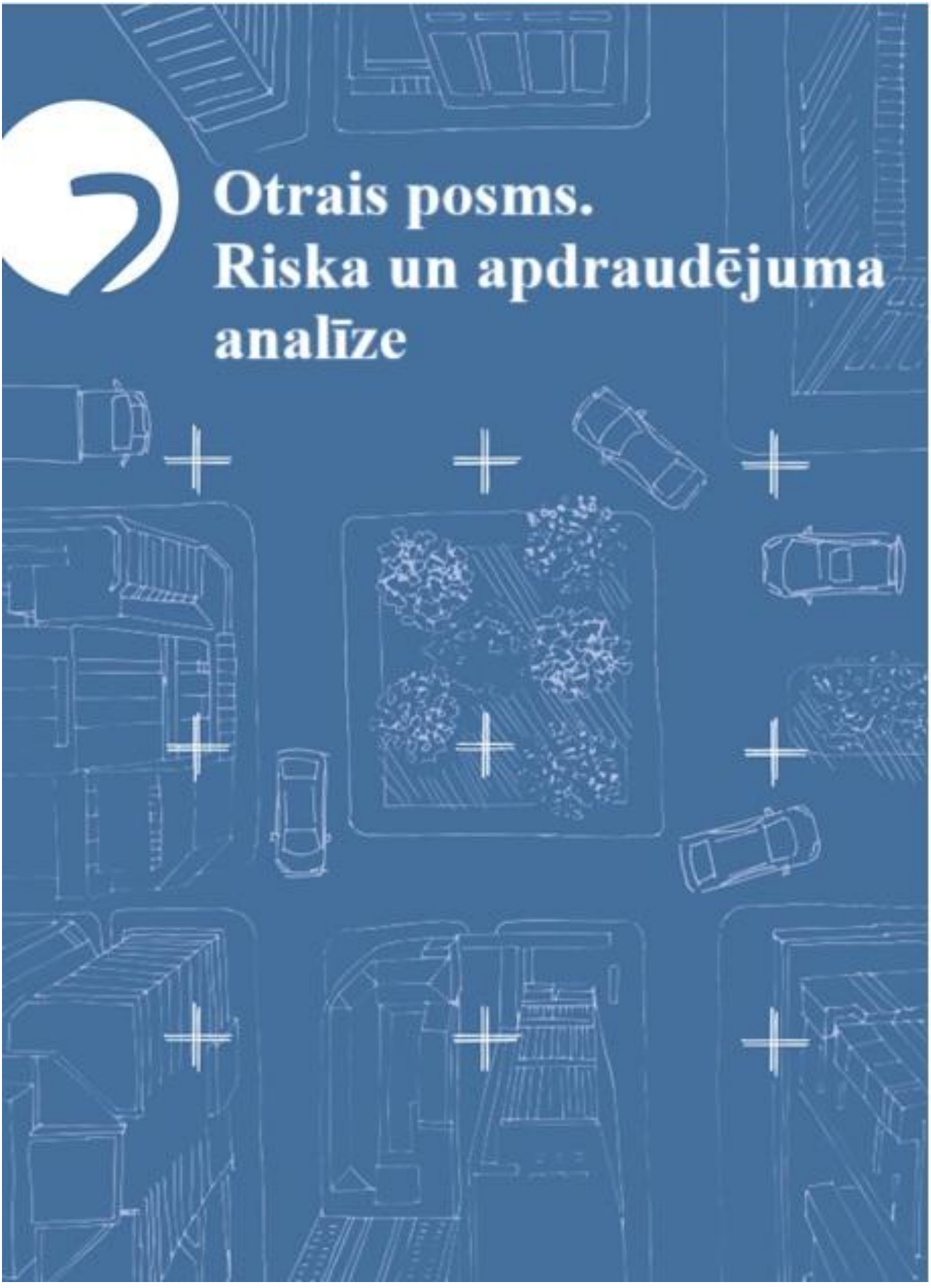
[11] Tumšās *UAS* jeb neredzamās *UAS* ir bezpilota lidaparāti, kas lido automātiskā lidojuma režīmā, neraidot *RF* signālus ne no tālvadības pults, ne arī no drona.

- **Kiberdrošība** ir svarīgs elements visos risinājumos, kuros ir IKT sistēmas, kurām ir interneta pieslēgums, vai kuros notiek informācijas apmaiņa ar citām sistēmām. *C-UAS* risinājumi jāizstrādā, izmantojot pieejamos kiberaizsardzības pasākumus. Visiem projekta elementiem jāspēj darboties bez interneta pieslēguma. Kad tiek identificēta augsta riska pakāpe, ja iespējams, jābūt pieejamām rezerves sistēmām un sensoriem.

3. IZCĒLUMS. SĀKUMA POSMA KOPSAVILKUMS

Šā posma beigās jums jābūt labākai izpratnei par turpmāk norādītajiem elementiem.

- Darbības pamatojums un skaidrs pilnvaru apraksts.
- Kas pret ko un kur ir jāaizsargā.
- Tehnoloģiju izmantošanas ierobežojumi pretpasākumu risinājumā.
- Nepieciešamība pēc *C-UAS* risinājuma ar definētām darbības vajadzībām un projekta pārvaldību. Šeit jāiekļauj skaidra darbības joma, mērķi un sasniedzamie rezultāti.
- Informācija par objektu un vides informācija, kas varētu ietekmēt *C-UAS* risinājumu.
- Ieinteresēto pušu analīze (augstā līmenī).
- Pamatpakalpojumu minimums, kas nodrošinās sagatavošanos un ieviešanu.


Otrais posms.
Riska un apdraudējuma analīze

Šajā posmā analizē aizsargājamā objekta *UAS* apdraudējumu. Šajā rokasgrāmatā izklāstītā pieeja *UAS* uzbrukumu riska novērtēšanai ir pamatota ar Starptautiskās Standartizācijas organizācijas (*ISO*) standartā 31000:2018[12] formulēto riska novērtējuma vispārīgo definīciju: "Riska novērtējums ir kopējais riska identificēšanas, riska analīzes un riska izvērtēšanas process". Šāda apraksta mērķis ir iekļaut riska procesā gan dabas, gan cilvēka ierosinātu apdraudējumu pat tad, ja ir ļoti grūti izvērtēt retu notikumu īstenošanās iespējamību un skaitliskā ziņā novērtēt sekas cilvēkiem/sociālajā jomā. *UAS* riskus ieteicams novērtēt, izmantojot riska novērtēšanas metodiku, ko objektā jau izmanto, un atjaunināt risku sarakstu, pievienojot apzinātos *UAS* riskus. Jau ieviestās metodikas izmantošana samazinās dublēšanu un novērsīs divu atšķirīgu riska novērtēšanas metožu nesaderību. Ja ir jāizstrādā jauns riska novērtēšanas process, *JRC* KI riska novērtējumā[13] ir vērtīgi norādījumi par to, kā piemērot *JRC* integrētas drošības pieeju[14]. Tāpēc otrajā posmā riska novērtējums ir kopsavilkums no *JRC* rokasgrāmatas par fizisku aizsardzību pret *UAS*.

Visos gadījumos riska novērtējumam ir jāpalīdz ieinteresētajām personām izprast konkrētos objekta *UAS* riskus, lai tās varētu izstrādāt *C-UAS* risinājumu, kas mazina apzinātos riskus.

4. IZCĒLUMS. OTRAIS POSMS. RISKS UN APDRAUDĒJUMS

Pirms šā posma uzsākšanas ir jāiegūst šādi elementi:
- objekta risku reģistrs (no iepriekšējiem un citiem saistītiem riska novērtējumiem);
- izpratne par valsts un ES[15] [16] noteikumiem un tiesību aktiem, kas attiecas uz KI vai sabiedrisko vietu, ko nepieciešams aizsargāt;
- augsta līmeņa prasības, kā definēts pirmajā posmā "Sākums";
- informācija par objektu un vidi.

Šā posma beigās jums jābūt izpildītiem šādiem elementiem:
- apdraudējuma identifikācija;
- objekta apsekojums;
- riska un apdraudējuma analīze;
- reaģēšanas plāns apdraudējuma gadījumā.

Analizētā *UAS* ļaunprātīgā izmantošana ir tikai viens no līdzekļiem, ko noziedzīga nodarījuma izdarītāji varētu izmantot, uzbrūkot indivīdam, sabiedriskai vietai vai infrastruktūrai. Iespējami dažādi uzbrukuma taktiskie paņēmieni, kuros izmanto *UAS* iespēju priekšrocības.

[12] International Organization for Standardization, ISO 31000:2018, Risk management – Guidelines, 2018.
[13] JRC risk assessment for critical infrastructure, https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en.
[14] https://home-affairs.ec.europa.eu/news/security-design-protection-public-spaces-terrorist-attacks-2022-12-14_en.
[15] Komisijas Deleģētā regula (2019. gada 12. marts) (ES) 2019/945 par bezpilota gaisa kuģu sistēmām un trešo valstu bezpilota gaisa kuģu sistēmu ekspluatantiem, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32019R0945.
[16] Komisijas Īstenošanas regula (2019. gada 24. maijs) (ES) 2019/947 par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32019R0947.

Lai atvieglotu izvērtēšanas procesu, ir ieteikta scenāriju izstrāde, ņemot vērā izvērtētās KI neaizsargātību. Turpmāk 10. attēlā parādīts riska novērtēšanas process.

- **Apdraudējuma identifikācijas** procesā identificē iespējamos uzbrukuma līdzekļus un metodes, tostarp nosakot izvērtētā aktīva neaizsargātību pret aplūkoto *UAS* uzbrukuma taktisko paņēmienu, novērtējot esošos aizsardzības pasākumus (ja tādi ir) un izstrādājot scenārijus.

- **Riska analīzē** novērtē katra apdraudējuma veida īstenošanās iespējamību un ietekmi, papildus apzinot visus neaizsargātības veidus un trūkumus, ko varētu izmantot. Riska analīzi var veikt ar dažādiem paņēmieniem, tostarp apmaiņu ar idejām, scenāriju analīzi vai matemātiskus modeļus. Riska analīzi veic, lai sniegtu visaptverošu izpratni par esošiem riskiem un identificētu visbūtiskākos riskus, kas jānovērš.

- **Riska izvērtējums** ir riska skaitliskā novērtējuma vai vērtējuma piešķiršana katram apdraudējuma veidam, pamatojoties uz tā īstenošanās iespējamību un iespējamo ietekmi. Riska izvērtējuma mērķis ir noteikt prioritārus riskus un noteikts, kuriem jāpievērš tūlītēja uzmanība. Riskus, kuru īstenošanās iespējamība ir visticamākā un kuru ietekme ir vislielākā, parasti uzskata par viskritiskākajiem, toties riskus, kuru īstenošanās iespējamība un ietekme ir zema, var uzskatīt par mazsvarīgākiem.

- **Riska apstrāde** ir atbilstīgu riska kontroles pasākumu noteikšana un ieviešana, piemēram, drošības protokolu īstenošana, katastrofu seku likvidēšanas plāna uzlabošana vai apdrošināšanas iegāde. Riska apstrādes mērķis ir samazināt iespējamā apdraudējuma īstenošanās iespējamību un ietekmi, kā arī mazināt organizācijas kopējo risku. Konkrēti riska apstrādes pasākumi tiks izvēlēti, ņemot vērā attiecīgo risku specifiku, pieejamos resursus un organizācijas riska pielaidi.

10. attēls. Riska pārvaldības posmi

Riska novērtēšanas rezultāts var ievērojami atšķirties atkarībā no pamatinformācijas, kas pieejama ekspertam, kurš novērtē risku. Ja scenārija īstenošanās iespējamības izvērtēšanai nav pietiekamu datu, riska novērtēšanai var pieņemt kvalitatīvu metodiku un izvirzīt spriedumus. Lai palielinātu objektivitāti, ekspertiem jāatbilst noteiktām prasībām, piemēram, jābūt pieredzei terorisma riska novērtēšanā, objektivitātei un nedrīkst būt interešu konflikti.

Riska novērtējums jādokumentē, pievienojot norādījumus par to precīzu interpretāciju izvērtētā aktīva īpašniekiem/pārvaldniekiem, kas atbild par pieņemamu riska pakāpes robežu noteikšanu un lemj, vai ir nepieciešama riska apstrāde.

Rūpīga apdraudējuma un riska analīze ir *C-UAS* risinājuma izstrādes procesa stūrakmens, jo tajā nosaka pamatprasības gan attiecībā uz paredzēto sistēmu, gan plašāku risinājumu. Apdraudējuma un riska analīzē izstrādātie scenāriji ir svarīga informācija, kas nepieciešama testēšanai ieviešanas posmā, kā arī regulārai testēšanai, izmantojot *C-UAS* risinājumu. Jāapzinās, ka visi risinājumi un izpratne par apdraudējumu laika gaitā mainīsies un ka šāda analīze regulāri ir jāatkārto. Analīzē ir skaidri jādefinē iespējamais kaitējums, ko nesadarbīgas *UAS* var radīt KI vai sabiedriskai vietai (apdraudējums), un tā īstenošanās iespējamība (risks).

Vairākumā gadījumu pašas *UAS* nerada atsevišķu risku, bet ir dala no plašāka riska (ko sauc par "makrorisku"). Tādēļ ir ieteicams *UAS* risku apstrādāt plašākā objekta riska pārvaldības programmā, nevis atsevišķā *UAS* riska novērtējumā.

2.1. RISKA IDENTIFIKĀCIJA

Riska novērtēšanas procesa pirmajā posmā nosaka izvērtētajam aktīvam atbilstošus *UAS* apdraudējuma veidus. Identificējot apdraudējumu, precīzi nosaka taktiskos paņēmienus, ko agresori varētu izmantot, un formulē iespējamos scenārijus. Cilvēka radītus apdraudējumus un to īstenošanās iespējamību ir grūti noteikt, jo, pretēji dabas stihijas riskiem, dati nav pietiekami, tāpēc, centieni konkrētus apdraudējumus saistīt ar iespējamo mērķi parasti ir lielā mērā subjektīvi. Datus par esošiem un potenciāliem draudiem, uzbrukuma nodomu vai citu saistītu sensitīvu informāciju var lūgt izlūkdienestiem un *LEA*. Vairāk informācijas par pieejamajiem datu avotiem, kas var atvieglot apdraudējuma noteikšanu, var skatīt dokumentā "Security by Design: Protection of public spaces from terrorist attacks" [Integrētā drošība Sabiedrisku vietu aizsardzība pret teroristu uzbrukumiem][17].

2.2. RISKA ANALĪZE

Kritisko infrastruktūru apdraudējuma veidi var ievērojami atšķirties. Objekta raksturlielumi (vide, lielums, blakus esošos objektos ieviesti risinājumi, ēkas utt.) ietekmē apdraudējuma kopainu. Turklāt katram objektam attiecībā uz *UAS* būs atšķirīgi apsvērumi. Piemēram, cietuma īpašnieks varētu vairāk domāt par kontrabandas piegādi ar *UAS*, toties publiska pasākuma organizētāji vairāk pievērsīsies *UAS* apdraudējumiem, kas varētu ietekmēt sabiedrības drošību. Visbiežāk iespējamās apdraudējuma kategorijas parādītas 5. attēlā.

Svarīgi ir identificēt tos objekta elementus, kurus varētu ietekmēt nesadarbīgu *UAS* uzbrukumi. Tostarp, bet ne tikai, ir cilvēki, ēkas, aktīvi, drošumam svarīgi pakalpojumi, KI pamatdarbības un kontrolēti materiāli.

[17] Coaffee, J. et al., *Security by Design: Protection of public spaces from terrorist attacks*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2022.

Lai gūtu pilnīgu ieskatu, ieteicams veikt objekta apsekojumu, kas ietver šādus elementus:

- **objekta specifika**, ieskaitot kritisko aktīvu atrašanās vietas un objekta piekļuves vietas;
- **vide**, ieskaitot objekta stāvokli trīsdimensiju attēlojumā, topogrāfiju, zemes izmantojumu (pilsēta, lauki, mežs) un cilvēku atrašanās vietas (pilsētas teritorijas, būves, transporta maršruti);
- **virtuālais apvidus**, ieskaitot gaisa telpas ierobežojumus, elektromagnētiskā vai *RF* spektra izmantošanu, potenciālās aklās zonas noteikšanu, kā arī aptvēruma izsekošanu un noteikšanu (piemēram, koki, kas traucē radara signālus);
- **iespējamās *UAS* palaišanas vietas un tuvošanās maršruti**, kas attiecas uz konkrētā infrastruktūras objekta vidi, ieskaitot tā ģeogrāfiju, procedūras un iespējas, kas noteiks situācijas apzināšanai piemērojamo metodiku;
- **fiziskā neaizsargātība**, piemēram, ēkas konstrukcijas un logi.

Pēc objekta apsekojuma tā rezultāti jāizmanto, lai izprastu apdraudējumu un iespējamās neaizsargātības veidus, kas, visticamāk, būs uzbrukuma mērķis. Ieteicams definēt katru scenāriju (nosakot spējas, nodomu, objekta apsekošanā konstatēto neaizsargātību) un pēc tam katru atsevišķi aprakstīt sīkāk (parasti atbildot uz šādiem jautājumiem: kas, ko, kur, kad, kāpēc, kā, kādas ir sekas utt.).

Lai skaitliskā izteiksmē noteiktu šo relatīvo iespējamību, ir jānovērtē apdraudējuma līmenis izvērtētā potenciālā mērķa apkārtnē. Tā kā parasti attiecīgie dati nav pietiekami un bieži vien to sensitīvās specifikas dēļ nav pieejami, tas ir sarežģīts uzdevums.

Turpmāk aplūkoti daži no rādītājiem.

- **Apdraudējuma vēsture.** Sniedz informāciju par iepriekš ziņotajiem, nesekmīgajiem vai novērstajiem uzbrukumiem/apdraudējumiem, kur izmantots katrs konkrētais taktiskais paņēmiens (attiecībā uz ēku, tās lietotājiem vai līdzīgos objektos). Apdraudējuma vēsturē ņem vērā teroristu grupu publiskos paziņojumus attiecībā pret civilajiem mērķiem un to motivāciju, jo īpaši, ja priekšroka tiek dota izvērtētajam scenārijam.
- **Uzbrukuma sarežģītība/iespējas.** Novērtē, kādas praktiskās/tehniskās speciālās zināšanas būtu nepieciešamas agresoram, lai veiktu uzbrukumu ar *UAS* (piemēram, izgatavojot improvizētu sprāgstierīci vai izmantojot ķīmiskas, bioloģiskas, radioloģiskas un kodolvielas), *UAS* iegādes grūtības (piemēram, atkarībā no tās lieluma), ierocis vai tā izveides komponenti. Izvērtē finanšu līdzekļus, kas nepieciešami materiālu iegādei vai citiem būtiskiem elementiem, kas varētu būt nepieciešami (piemēram, atbalsta infrastruktūra, sakaru tīkls, piegādes ķēde).
- **Pievilcīgums/motivācija.** Atkarīgs no mērķa pievilcīguma (piemēram, kultūras/reliģiskā/simboliskā nozīmē, cilvēku klātbūtne) saistībā ar iespējamo uzbrukuma taktiku. Izpēta, vai noteikts darbības veids uzbrucējam šķiet pievilcīgāks, jo aktīva funkciju dēļ tam varētu būt lielāka ietekme (piemēram, mijiedarbība ar citiem objektiem, papildu sekas valstij un sabiedrībai, publikas un/vai sensitīvu datu esība).

Iekļaujot *UAS* apdraudējumu scenārijos, pēc tam tos var izmantot makrorisku kartēšanai. Turpmāk uzskaitīti *UAS* izraisītie makrorisku piemēri.

- **Ievainojumi/nāve.** Tostarp *UAS* kā ieroču izmantošana fiziskā uzbrukumā.
- **Kontrolētu materiālu zaudējums.** *UAS* izmantošana noziedzīgu darbību atbalstam (piemēram, intelektuālais īpašums, kritiski svarīga uzņēmējdarbības informācija vai kontrolētu vielu zādzība).
- **KI darbību kritiska izjukšana/traucēšana.** *UAS* izmantošana, lai veiktu sabotāžu tieši pret KI objektu vai netieši pret saistītu objektu, kas ir bruņots un/vai kam ir atbalsta funkcija (piemēram, izlūkdatu vākšana /kiberuzbrukums).
- **Datu zaudējums.** *UAS* izmantošana, veidojot izlūkošanas platformu, kas atbalsta naidīgu darbību plānošanu, spiegošanu un nelikumīgu informācijas vākšanu.

Minēto makrorisku kartēšana atbilstīgi noteiktajiem *UAS* apdraudējuma veidiem katram KI objektam būs atšķirīga. Saimnieciskās darbības īpašniekiem ir jānovērtē, kā makroriski ir saistīti ar viņu objekta *UAS* apdraudējuma veidiem. Visos ieviestajos risinājumos visi makroriski noteikti būs sasaistīti atšķirīgi.

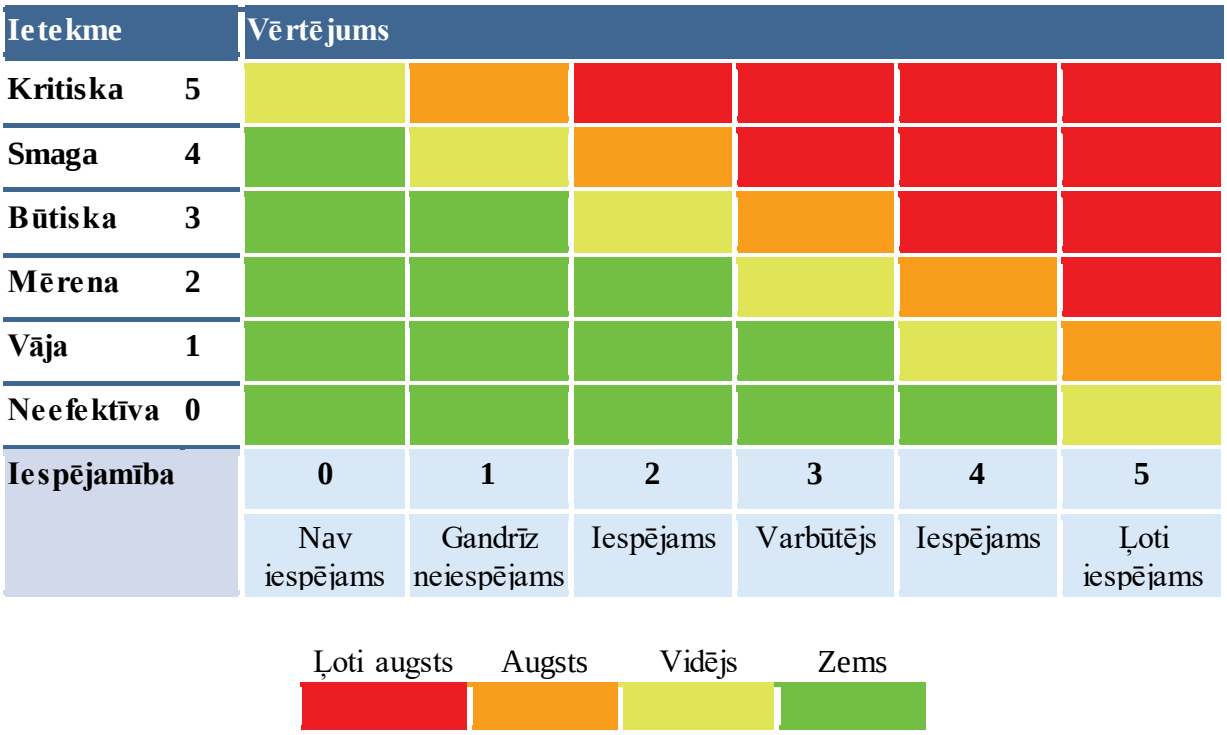
Piemēram, *UAS* apdraudējuma veids "fizisks uzbrukums" varētu būt saistīts ar "nāves" risku. Riska vadībā var izmantot *UAS* risku reģistru, lai izvērtētu scenārijus. Jānorāda, ka riska matrica ir jāpielāgo atbilstīgi konkrētajam KI objekta kontekstam. Tas ar piemēru ir parādīts 11. attēlā.

11. attēls. Piemērs ar *UAS* apdraudējuma veidiem, kas kartēti atbilstīgi makroriskiem

UAS incidentu iespējamības un seku novērtējums

Ļaunprātīgu *UAS* riska līmeņa novērtēšana ietver gan katra identificētā scenārija īstenošanās iespējamības izvērtējumu, gan potenciālās sekas šā scenārija īstenošanās gadījumā. Šajā procesā izmanto apdraudējuma un neaizsargātības novērtējumu rezultātus. To var attēlot riska matricā, kā parādīts 12. attēlā.

12. attēls. Riska matricas piemērs



Kad *UAS* riski ir identificēti *UAS* risku reģistrā, riska analīzes ietvaros var noteikt riska skaitliskā novērtējuma atsauces vērtību. Riska analīzē jāņem vērā turpmāk norādītie faktori.

- **Apdraudējuma faktori.** No apdraudējuma analīzes jānosaka iespējamie apdraudējuma izraisītāji. Tas ir svarīgs solis, lai izstrādātu iespējamos scenārijus, kuriem jāveic riska kontroles pasākumi.
- **Iespējamība.** Kvalitatīvs, relatīvs vērtējums, ņemot vērā apdraudējuma izdarītāja motivāciju un iespējas. Vērtējumu parasti iedala no 0 līdz 5 (5 ir viskritiskākais apdraudējums) vai no "neiespējams", "vidēji iespējams", "ļoti iespējams", "iespējams" līdz "gandrīz noteikti".
- **Ietekme.** Vērtējuma pamatā ir apdraudējuma ietekme uz attiecīgajiem KI makrorisku reģistrā noteiktajiem riskiem. Kvalitatīvo novērtējumu ieteicams veikt, izmantojot piemērotu metodiku un atsevišķu KI saimnieciskās darbības īpašnieku saskaņotu vērtēšanas sistēmu[18].
- **Riska skaitliskais novērtējums.** Riska skaitlisko novērtējumu aprēķina, iespējamību un ietekmi reizinot ar iespējamo svara koeficientu, pamatojoties uz KI objekta riska pieņemšanas līmeņiem. Riska skaitliskais novērtējums var būt lineāri svērts, ja notikuma ietekme var būt nesamērīga attiecībā pret iespējamību (zemas iespējamības notikumi var būt pietiekami katastrofāli, lai būtu nepieciešami atbilstīgi riska mazināšanas pasākumi). Lai gan šajā rokasgrāmatā ir aplūkota viena riska aprēķināšanas iespēja, lasītājs var brīvi izvēlēties metodiku un/vai izmantot to, kas objektā jau ir ieviesta.

[18] Viens piemērs varētu būt vērtības, kas saistītas ar uzņēmējdarbības nepārtrauktības plānu (piemēram, normāla stāvokļa atjaunošanas punkta mērķis, normāla stāvokļa atjaunošanas laika mērķi vai darbības atjaunošanas laiks).

Uzbrukuma sekas ir saistītas ar aktīva veidu un apstākļiem incidenta brīdī. Iepriekš notikuši incidenti ir pierādījuši, ka tieša, tūlītēja uzbrukuma ietekme var būt gan saistīta ar cilvēka dzīvību (piemēram, ievainojumi vai nāves gadījumi), gan lieliem ekonomiskiem zaudējumiem (piemēram, remonta izmaksas un pakalpojumu sniegšanas traucējumi), gan arī vides katastrofām (piemēram, ūdens piesārņojums). Netiešas ilgtermiņa sekas ir grūtāk novērtēt, jo tās ietver tādus politiskus/sociālus aspektus kā ietekme uz iedzīvotāju psiholoģisko stāvokli un netiešas ekonomiskās izmaksas (piemēram, ietekme uz tūrisma nozari). Lai atvieglotu šo izvērtēšanu, vērtētājam ir jāatbild uz vairākiem, tostarp turpmāk norādītajiem, jautājumiem.

- Cik cilvēku būtu nogalināti vai ievainoti pēc uzbrukuma, kurā izmantots *UAS* taktiskais paņēmiens?
- Kādi pakalpojumi uzbrukuma gadījumā tiktu traucēti? Cik ilgi turpināsies traucējumi? Vai attiecīgie pakalpojumi tiek dublēti un kādas būs remontdarbu izmaksas?
- Vai mijiedarbībā ar citiem aktīviem vai pakalpojumiem uzbrukums izraisīs kaskādes efektu?
- Kādas ir sagaidāmās remonta izmaksas? Vai ir pieejamas aizstāšanas iespējas?
- Vai KI ir kritiskā komunālā infrastruktūra vai sensitīva informācija, ko varētu apdraudēt? Kāda ir to zuduma vai pakalpojuma traucējumu netieša ietekme?
- Vai organizācijai/īpašniekam pastāv politisku seku, reputācijas kaitējuma un/vai drošības pārkāpumu (piemēram, personas datu aizsardzības pārkāpumi) iespējamība?
- Kādas ir netiešās ekonomiskās izmaksas (piemēram, tūrisma nozarei) un kāda ir ietekme uz iedzīvotāju psiholoģisko stāvokli?

2.3. RISKA IZVĒRTĒJUMS

UAS risku izvērtē pēc *UAS* riska analīzes. Pēc aprēķināšanas, pārskatīšanas un saskaņošanas atsauces riski pēc tam ir jānovērtē atbilstīgi riska pieņemšanas līmeņiem, lai noteiktu, vai ir nepieciešami papildu pasākumi riska mazināšanai. Katrs risks jāizvērtē saistībā ar pieņemamības līmeņiem, salīdzinot ar KI saimnieciskās darbības īpašnieka apstiprināto pielaides līmeni. Riska skaitliskos novērtējumus, kas pārsniedz šo robežvērtību, uzskata par nepieņemamiem, un ir jāveic attiecīgi pasākumi.

Kā parādīts 13. attēlā, ir jāizvērtē pieci riska apstrādes risku elementi un katram riskam ir jāizvēlas iespējamā rīcība. Riski ir jāizvērtē, lai izvēlētos kādu no norādītajām darbībām.

13. attēls. Pieci riska apstrādes elementi

2.4. RISKA APSTRĀDE

Atbilstīgu lēmumu par *C-UAS* pieņemšana balstās uz izpratni par pamatsituāciju, taktiskā līmeņa tehnisko analīzi (par *UAS* darbību un/vai fizisko un elektromagnētisko *UAS* konfigurāciju) un piemērojamiem tiesību aktiem.

Attiecībā uz *UAS* pārtveršanu *C-UAS* risinājumā ir vairāki elementi, kas jāapkopo, lai pieņemtu lēmumu par pārtveršanu. Starp tiem ir apdraudējuma novērtējums, reglamentējošie un juridiskie parametri un pārtveršanas pilnvarojums.

Šis iedaļījums atspoguļo lēmuma pieņemšanas procesu, ko KI un sabiedrisko vietu īpašnieki var izmantot, lai noteiktu pareizo rīcību, kad ir konstatēts apdraudējums. Lēmuma pieņemšanas process lielā mērā ir saistīts ar sagaidāmo apdraudējumu un iespējamiem pretpasākumiem, ko var izmantot. Minētais iedaļījums atspoguļo KI reakciju uz *UAS* uzbrukumu un tāpēc ir galvenais līdzeklis virzībā uz *C-UAS* risinājuma izstrādi.

Sīki izstrādātais riska novērtējums ir jādokumentē, lai to vēlāk varētu izmantot nākamajos posmos.

5. IZCĒLUMS. RISKA UN APDRAUDĒJUMA ANALĪZES POSMA KOPSAVILKUMS

Šā posma beigās jums jābūt labākai izpratnei par šādiem elementiem:

- apdraudējuma izpratne;
- apdraudējuma scenāriju izpratne;
- identificēti konkrēti attiecīgā objekta *UAS* apdraudējuma veidi;
- identificēta objekta neaizsargātība;
- objekta apsekojums ar informāciju par kritisko aktīvu atrašanās vietām;
- apzināto risku mazināšanas plāns;
- riska matrica;
- apstiprināti riska pieņemšanas līmeņi;
- reaģēšanas plāns apdraudējuma gadījumā.

3 Trešais posms. *C-UAS* risinājuma izstrāde

C-UAS risinājuma izstrādes posms ir process, kurā izvēlas atbilstīgus riska mazināšanas pasākumus un tehnoloģijas, kas atbilst apzinātajiem riskiem un objekta un ieinteresēto personu vajadzībām.

Visiem risinājumiem kopīgi ir pamatpakalpojumi (skat. ievaddaļu), kas, mainoties vajadzībām, atvieglo riska mazināšanas līmeņu paaugstināšanu un pazemināšanu (piemēram, *VIP* apmeklējumi, tādi īslaicīgi pasākumi kā Ziemassvētku tirdziņi, lieli sporta pasākumi un koncerti). Riska mazināšana papildus pamatpakalpojumiem ir atkarīga no daudziem faktoriem, kas tiks aplūkoti šajā iedaļā. Mērķis ir pilnīga risinājuma ieviešana.

6. IZCĒLUMS. TREŠAIS POSMS. IZSTRĀDES POSMS

Šajā posmā nepieciešamā informācija:

- precīzs izstrādājamā risinājuma prasību apraksts (objekta vajadzības, mērķi un darbības joma);
- objekta risku reģistrs;
- precīzs reaģēšanas plāns apdraudējuma gadījumā;
- izpratne par tiesību aktu prasībām;
- augsta līmeņa prasības;
- informācija par objektu un vidi.

Šā posma beigās jums jābūt izpildītiem šādiem elementiem:

- objekta vajadzībām atbilstīgs projekts;
- augsta līmeņa risinājuma arhitektūra;
- atjaunināts objekta apsekojums;
- risinājuma ieviešanas specifikācijas;
- atjaunināta ieinteresēto personu analīze, nosakot konkrētas funkcijas un pienākumus.

Risinājuma izstrāde ir sarežģīts posms, un tas kļūs par pamatu ieviešanas un darbības posmiem. Lai gan *C-UAS* risinājumiem var būt daudz kopīgu faktoru, ikvienam elementam un uzstādījumam jābūt pielīdzinātam atbilstīgi riska pieņemšanas līmeņiem, objekta specifikai, pieejamajam budžetam utt. Būs nepieciešams skaidrs augstākā hierarhijas līmeņa, iestāžu un KI regulatoru pilnvarojums. Labs projekts un metodika palīdzēs vieglāk izdarīt izmaiņas, kad tas būs nepieciešams. Labs projekts palīdzēs arī iekļaut un pārvaldīt visos līmeņos iesaistīto ieinteresēto personu procesus un procedūras.

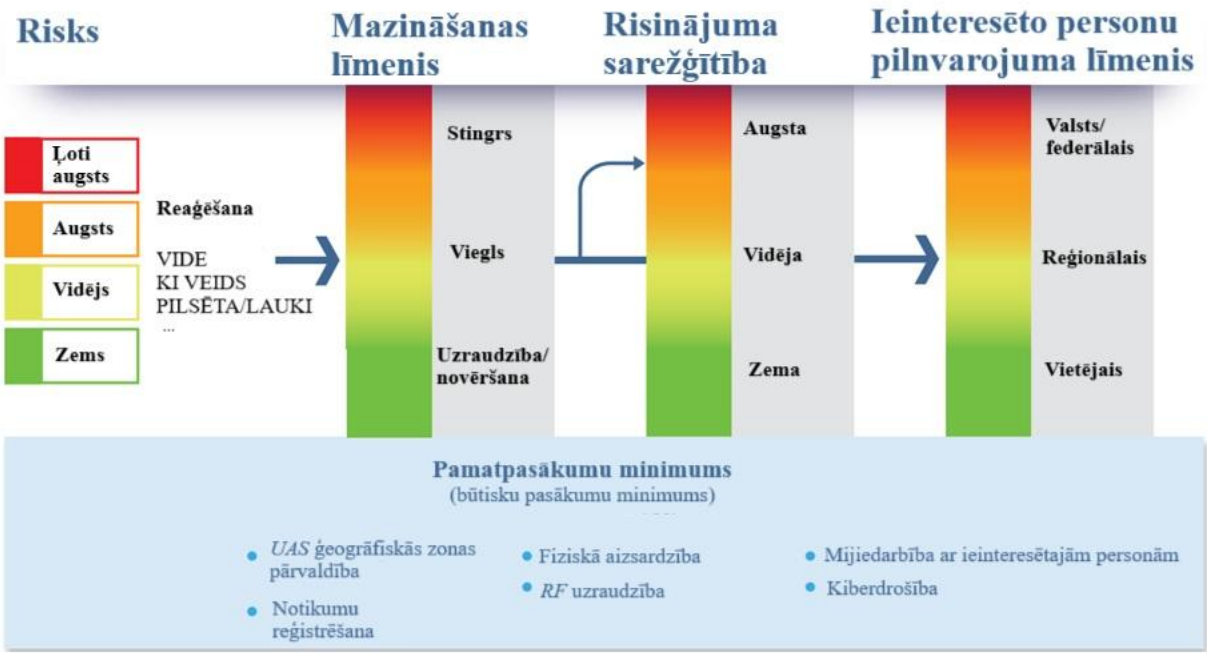
PADOMS

C-UAS risinājuma mērķis ir mazināt objektam radīto *UAS* risku ar atbilstīgiem pasākumiem, ievērojot juridiskos, tehniskos ierobežojumus un iesaistot vajadzīgās ieinteresētās personas.

Vienkāršotu risinājuma izstrādes procesa ceļvedi var apkopot četros galvenajos posmos, skat. 14. attēlu.

1. Riska novērtēšana un vides ierobežojumu un saimnieciskās darbības vajadzību apkopošana.
2. Problēmai piemērota riska mazināšanas līmeņa izvēle, ievērojot juridiskos ierobežojumus.
3. Izvēlētajam riska mazināšanas pasākumam atbilstīgu tehnoloģiju un risinājumu atlase.
4. Procesu un procedūru noteikšana kopā ar iesaistītajām ieinteresētajām personām un to īstenošana. Tādējādi ieinteresētās personas tiks iesaistītas visos līmeņos.

14. attēls. *C-UAS* izstrādes procesa ceļvedis



Izstrādes posma beigās objektam ir risinājuma prasību specifikācija, proti, plānotā risinājuma apraksts, iekļaujot ar to saistītās procedūras un procesus. Tas var būt pamats risinājuma iepirkuma procesam.

Turpmāk norādīti daži svarīgi elementi, kas jāapsver un jāizlemj izstrādes posmā.

- **Ieguldījuma pieeja.** Šajā posmā jāpieņem lēmums par projekta pirmā posma finansēšanu. Vairākumā risinājuma projektu, iespējams, būs jāpiesaista *C-UAS* eksperti. Lai mazinātu aizspriedumus pret risinājumiem, kurus tehnoloģiju uzņēmums jau ir ieviesis, daudzos gadījumos būtu lietderīgi nošķirt konsultantus un tehnoloģiju nodrošinātājus. Labam projektam jābūt pietiekami sīki izstrādātam, lai iepirkuma procedūrā to varētu izmantot kā tehnisko dokumentu. Jāapsver, vai risinājums tiks **iepirkts**, **nomāts** vai tiks iegādāts **kā pakalpojums**. Turklāt **izmaksu tāmi** ieteicams izstrādāt, ņemot vērā dažādus izmaksu faktorus (tostarp kā iekšējo, tā ārējo pušu izmaksu tāmes), kā arī to, kā risinājums darbības laikā tiks pārvaldīts un finansēts.
- **Juridiski apsvērumi.** To starpā ir atklāšanas un riska mazināšanas tehnoloģiju izmantošanas atļaujas. Jāizpēta arī tas, kādas ir iespējas attiecībā uz iejaukšanos objekta teritorijā un objekta perimetra apkārtnē. Tādēļ būs jāiesaista daudzas ieinteresētās personas, piemēram, *LEA*, iestādes, blakus esoši objekti, citu risinājumu pārvaldnieki,

gaisa telpas pārvaldības, *UTM*, gaisa satiksmes pārvaldības un *U-Space* operatori. Galu galā risinājumam ir jānodrošina, ka ir atrisināti un dokumentēti visi risinājuma aspekti, tostarp visas nepieciešamās risinājuma **atļaujas un licences**.

- **Risinājuma darbības joma un mērķis.** Ikvienā projektā ir svarīgi noteikt darbības jomu un mērķus, lai novērstu neskaidrības, pārpratumus un darbības jomas izplūšanu. Tas jādara, lai izvairītos no izdevumu pieauguma un neefektīvas īstenošanas, kas neatbilst attiecīgajām vajadzībām, vai lai izvairītos no tāda risinājuma pieņemšanas, kuru nevar mainīt vai integrēt, kad nepieciešamas izmaiņas.
- **KI, sabiedrisko vietu un apkārtnes attīstība.** Projektā jāņem vērā objekta un tā apkārtnes attīstība. Tas ietvers iekārtas citos objektos, kas varētu ietekmēt identifikācijas sistēmas.
- **Informācijas apmaiņa.** Ieinteresētajām personām ir jāapspriežas un jāvienojas par informācijas apmaiņu. Tas ir svarīgi attiecībā uz izmēģinājuma lidojumiem, kurus varētu atklāt apkārtnē ieviestie risinājumi, *UAS* ģeogrāfisko zonu un brīdinājuma zonu pārklāšanos, traucējumiem no identifikācijas sistēmām (piemēram, radara frekvencēm), *UAS* darbības attīstības tendencēm un iniciatīvām gaisa telpas pārvaldībai (*U-space* pakalpojumi un *UTM* sistēmu ieviešana) u. c.
- **Blakus iedarbības novērtēšana.** Šis ir ļoti svarīgs punkts, ko nedrīkst novērtēt par zemu. Jāpārbauda, kāda būs izvēlēto atklāšanas un neitralizēšanas tehnoloģiju iedarbība uz objektu, tā vidi, citām iekārtām, apkārtnē ieviestajiem risinājumiem u. c. Pārbaudē jo īpaši jāpievēršas riska mazināšanas pasākumu iedarbībai. Vairākumā gadījumu frekvences, ko izmanto sakariem starp zemes stacijām un bezpilota lidaparātu, ir tās pašas frekvences, ko parastās rūpniecības un mājsaimniecības ierīces izmanto bezvadu sakaru tīklam. Turklāt globālās navigācijas satelītu sistēmas signālu traucēšanai vai viltošanai var būt nevēlama blakus iedarbība.
- **Objekta apsekojums.** Projektā ļoti svarīgs ir precīzs un pilnīgs objekta un apkārtnes pārskats. Jāveic visaptverošs apsekojums, kas iekļauj ēku augstumu, kokus, ainavu u. c. To var izmantot, lai imitētu, izraudzītos un plānotu atklāšanas sensoru un neitralizācijas sistēmu izvietojumu. Otrajā posmā izmantotais objekta apsekojums (riska un apdraudējuma analīze) ir saistīts ar risku sarakstu ceturtajā posmā (zonas lieluma noteikšanas risinājuma ieviešana). Šim apsekojumam jābūt pietiekami precīzam un detalizētam, lai trešās puses to varētu izmantot risinājuma ieviešanai.

3.1. PAMATPASĀKUMU MINIMUMS

Pamatpasākumu minimumam jābūt visu risinājumu pamatā. Kā aprakstīts ievaddaļā, tie būs pamats visiem pārējiem pakalpojumiem un atvieglos nepieciešamo izmaiņu izdarīšanu. Daži no tiem jau var būt ieviesti, īstenojot parastos drošības procesus, un pēc tam tie būs jāatjaunina, pievienojot *C-UAS* elementus. Nākamajā iedaļā aprakstīti pakalpojumi un ieteikumi attiecībā uz to ieviešanu.

***UAS* ģeogrāfiskās zonas pārvaldība**

Apkārt aizsargātajam objektam ir lietderīgi noteikt dažādas zonas, kurās notiek atšķirīgas darbības. Lai noteiktu šīs zonas, svarīgi faktori ir aizsargājamās teritorijas vide, atrašanās vieta un veids Novērojamā teritorija un tās lielums jānosaka, ņemot vērā apdraudējumu, pret ko ir jāaizsargā. Konstatētie fakti būs svarīgi faktori, lai noteiktu to zonu lielumu, kurās izvietoti sensori, kā arī to, kur un kādas darbības jāveic. Jo lielākas zonas, jo grūtāka un dārgāka to aizsardzība. Katram ieviestajam risinājumam zonu konfigurācija un skaits var

atšķirties. Galu galā tās jāprojektē tā, lai būtu pietiekami daudz laika reaģēšanai un neitralizēšanai, radot vismazāko netiešo bojājumu apjomu. Zonas jāplāno tā, lai būtu aizsargātas visas objekta daļas vai lielākā daļa augsta riska daļu. Nosakot šīs zonas, jāapsver, kādas pilnvaras ir nepieciešamas, lai neitralizētu apdraudējumu, un kam ir šādas tiesības. Daudzos gadījumos katrai zonai var būt atšķirīgi dalībnieki. Tāpēc procesu un procedūru projektā jāiekļauj visi dalībnieki. Tādēļ ir svarīgi precīzi analizēt vajadzības un skaidri definēt procesus un procedūras *C-UAS* drošības zonās un to apkārtnē.

Vēlams ieviest vairākus zonu slāņus, kā parādīts 15. attēlā. To definīcijas un lielums jāpielīdzina riska mazināšanai nepieciešamajiem pasākumiem, apstiprinātajiem mazināšanas pasākumiem un jāsaskaņo ar risinājumā iesaistītajām ieinteresētajām personām. Sensoru izvietojums ir cieši saistīts ar noteikto lielumu un zonās paredzēto darbību definīcijām (skat. informāciju 3.2. iedaļā attiecībā uz apsvērumiem par sensoru izvietojumu un par to, kas jāņem vērā, lai visās zonās iegūtu pareizu pārklājumu).

Zonu lielums un tām piesaistītās darbības jānosaka tā, lai visiem iesaistītajiem dalībniekiem būtu laiks saskaņoti mazināt *UAS* incidentu. Mazināšanas vietai jābūt cik vien iespējams aizsargātai un drošai, lai radītu minimālus netiešos bojājumus un ievērotu noteikumus un tiesisko regulējumu.

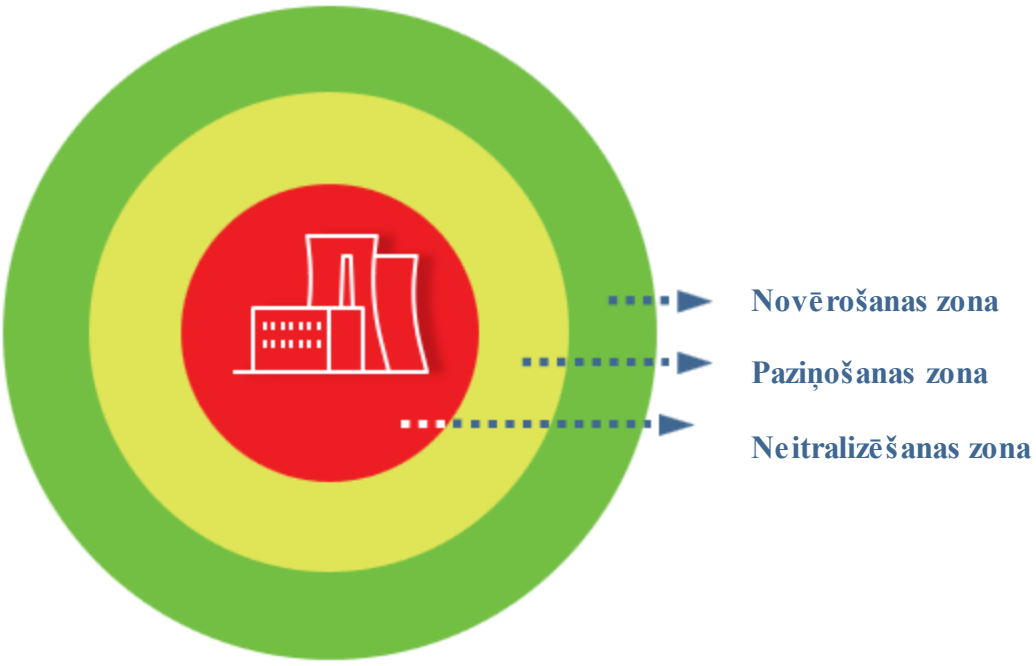
***UAS* ģeogrāfiskā zona** ir gaisa telpa, kuru valsts civilās aviācijas iestāde var piešķirt objekta īpašniekam, lai varētu noteikt *UAS* ekspluatācijas noteikumus[19]. Tie var būt *UAS* specifikāciju minimums, paziņojumi, laika ierobežojumi, ekspluatācijas vietas u. c. Tā ir arī zona, kurā zonas pārvaldītājam būs atļauja iejaukties konstatēto lidojumu gadījumā. Atkarībā no valsts un vietējiem noteikumiem tie varētu būt arī mazināšanas pasākumi. Tādēļ ir ļoti svarīgi ieviešamo darbību izstrādē un definēšanā iesaistīt arī regulatīvās iestādes.

C-UAS daudzpakāpju zonu modelis

- Iekšējais slānis it **neitralizēšanas zona**. Tā ir *UAS* ģeogrāfiskās zonas trīsdimensiju zona, kurā KI vai sabiedriskās vietas īpašnieks vēlas neitralizēt ikvienu neatļautu *UAS* ar pasākumiem, kas noteikti apzināto risku mazināšanai. Šīs zonas izmēru ir svarīgi noteikt pareizi, lai neitralizācijas dalībniekiem nepieciešamības gadījumā būtu attiecīgās juridiskās pilnvaras un reaģēšanas laiks. Šajā zonā jābūt pilnīgam identifikācijas sistēmu pārklājumam.
- **Paziņošanas zonā** apdraudējums tiek rūpīgi uzraudzīts, un īstenošanās gadījumā visi dalībnieki gatavojas mazināšanai, ievērojot noteiktos procesus un procedūras. Šīs zonas lielums ir atkarīgs no laika, kas nepieciešams, lai piesaistītu resursus un sagatavotos iekļūšanai zonās, kurās nepieciešama neitralizācija.
- **Novērošanas zona** ir teritorija ap novērošanas zonu. Šo zonu izmanto, lai novērotu darbības, ar kurām var optimizēt risinājumu un situācijas apzināšanos. Šajā zonā var būt daļējs identifikācijas sistēmu pārklājums.

[19] Komisijas Īstenošanas regula (2019. gada 24. maijs) (ES) 2019/947 par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām.

15. attēls. *C-UAS* daudzpakāpju zonu modelis



Turpmāk izklāstīti vairāki svarīgi apsvērumi par minētajām zonām.

- *UTM* sistēmas **iekļaušana** un izmantošana ir svarīgs rīks, ko izmantot gaisa telpas pārvaldībai un *U-Space* un apkārtnes iekļaušanai. Vienota *UTM* pakalpojuma izmantošana (piemēram, no mākoņa) sniedz vērtīgu papildu informāciju jebkuram risinājumam, **taču *UTM* nav *C-UAS* risinājums**.
- Ja *UAS* izmantošana ir paredzēta objektā vai aizsargājamā zonā, ir jāizpēta un jāplāno, kā to pārvaldīt un integrēt *C-UAS* risinājumā.
- Jau agrīnā risinājuma izstrādes posmā prasiet atbildīgajai civilās aviācijas iestādei *UAS* ģeogrāfisko zonu un gaisa telpas pārvaldību.
- Informējiet ieinteresētās personas un apkārtējos objektus par šīs *UAS* ģeogrāfiskās zonas ieviešanu.
- Vairākumā gadījumu būs lietderīgi reģistrēties kā *UAS* ekspluatantam (kā definēts ES tiesību aktos[20] [21]), lai saņemtu atļauju veikt izmēģinājuma lidojumus, mācības, apsekojumus, u. c.
- Pārliecinieties, ka visas objekta apdrošināšanas polises ir atjauninātas, lai iekļautu visu veidu *UAS* izmantošanu aizsargājamajā objektā un ap to. Tas jādara, lai veiktu objekta apsekojumu, verificētu sensorus, veiktu ielaušanās testus, mācības u. c.
- *C-UAS* sistēmas veiktspējas verifikācijas un validācijas testi ir jāizstrādā atbilstīgi apdraudējuma scenārijiem, un tiem ir jāatbilst nepieciešamās aizsardzības mērķim. Piemēram, nav lietderīgi veikt augsta līmeņa teroristu uzbrukuma testu risinājumā, kas izstrādāts, lai aizsargātu pret privātuma pārkāpumiem, uzraudzība nav neitralizēšanas metode.

[20] Komisijas Deleģētā regula (2019. gada 12. marts) (ES) 2019/945 par bezpilota gaisa kuģu sistēmām un trešo valstu bezpilota gaisa kuģu sistēmu ekspluatantiem.
[21] Komisijas Īstenošanas regula (2019. gada 24. maijs) (ES) 2019/947 par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām.

- Zīmes apkārt objektam jāuzstāda saskaņā ar vienošanos, kas panākta ar iestādēm un apkārtējiem objektiem. To varētu sasaistīt ar informācijas kampaņu, lai apkārtējām ieinteresētajām personām paziņotu, ka attiecīgā zona nav *UAS* lidojumu zona.
- Pārvaldības procesus un procedūras ieviesiet iekšēji un kopā ar ieinteresētajām personām (piemēram, *UTM*, vietējām ieinteresētajām personām, *LEA*, iestādēm).

Notikumu reģistrēšana

Lai uzturētu risinājuma efektivitāti un lietderīgumu, ir svarīgi reģistrēt notikumus. Projektam jābūt pietiekami elastīgam, lai varētu reģistrēt manuālus novērojumus, sensoru novērojumus un informāciju, kas saņemta no ārējiem avotiem, piemēram, *UTM* vai blakus esošajiem objektiem. Ierakstu uzglabāšanas laiks jānosaka tā, lai tos varētu izmantot tendenču noteikšanai. Ierakstu analīze jāveic ik pēc noteikta laika un jāizmanto, lai atjauninātu/modernizētu risinājumu.

Reģistrētajai informācijai jābūt pietiekamai, lai noteiktu tendences un identificētu iespējamus jaunus apdraudējumus (piemēram, ja kāds mēģina noskaidrot, vai objektā ir ieviesta aizsardzība pret *UAS*). Šāda informācija varētu ietvert atklāšanas gadījumus, kas nav verificēti kā *UAS* vai ir klasificēti kļūdaini. Reģistrēšana ir jācentralizē no visiem avotiem, kuriem ir pēc iespējas pilnīgāka informācija, un to piemēri norādīti turpmāk.

- Tiešā un tīkla attālinātā ID, kā definēts Komisijas Deleģētajā regulā (ES) 2019/945 (*UAS* ekspluatanta reģistrācijas numurs un verifikācijas kods, unikāls bezpilota lidaparāta sērijas numurs, laika zīmogs, *UAS* ģeogrāfiskā atrašanās vieta, ātrums, maršruts, pilota atrašanās vieta, pacelšanās atrašanās vieta un ārkārtējs stāvoklis).
- Informācija par *UAS* un visa pieejamā informācija (videspiekļuves vadības adrese, bezpilota lidaparāta tips, sērijas numurs u. c.).
- Kas atklāja – detektori, cilvēki, metodes u. c.
- Attēli, videomateriāli un signāla informācija, kas paredzēta izmantošanai tiesu ekspertīzē. Informācijas ievadītājs (piemēram, ārēja novērošana, *UTM*, cits *C-UAS* risinājums, sensors un detektors). Informācija par laiku un atrašanās vietu.
- Lidojuma informācija un parametri.
- Apstiprināti un neapstiprināti lidojumi.
- Mazināšanas pasākumi: ja sistēma veic kādus pasākumus, lai mazinātu atklāto apdraudējumu, piemēram, *UAS* sakaru sistēmas traucēšanu vai pārvirzīšanu, šīs darbības ir jāreģistrē, norādot arī veiktās darbības laiku un veidu.
- Viltus trauksmes: jāreģistrē visi viltus trauksmes gadījumi, ko aktivizējusi sistēma, norādot šādas trauksmes iemeslu un visus korektīvos pasākumus, kas veikti, lai turpmāk nepieļautu viltus trauksmes.
- Sistēmas veiktspēja: sistēmas veiktspējas rādītāji, jāreģistrē, piemēram, atklāšanas ātrums un reakcijas laiks, lai pastāvīgi uzraudzītu sistēmas efektivitāti.
- Lietotāju darbības: jāreģistrē visas darbības, ko veic *C-UAS* risinājuma sankcionētie lietotāji, norādot darbības laiku un specifiku, kā arī lietotāja identitāti.
- Sistēmas kļūdas: jāreģistrē visas sistēmas kļūdas vai darbības traucējumi, kā arī diagnostikas informācija, ko var izmantot traucējummeklēšanā un problēmas atrisināšanā.
- Operatora darbības.

Visai reģistrētajai informācijai jābūt eksportējamai, lai attiecīgās iestādes to varētu izmantot tiesu ekspertīzē.

Fiziskā aizsardzība

Fiziskā aizsardzība[22] ir svarīgs dažādu *UAS* radītu apdraudējuma veidu mazināšanas pasākums, tomēr tam bieži vien nepievērš pietiekamu uzmanību, un tas ir rūpīgi jāizvērtē. Dažos gadījumos fiziskās aizsardzības pasākumu ieviešana varētu būt vienkāršāka, lētāka un ātrāka nekā dārgo *C-UAS* sistēmu ieviešana.

Daži piemēri:

- plēves uz logu stikliem, lai aizsargātu pret apdraudējumu, ko rada mazas *UAS*, ietriecoties logos;
- plēves uz logu stikliem, lai nepieļautu filmēšanu no ārpuses;
- tīkli virs cilvēkiem, lai nepieļautu cilvēku ievainošanu;
- ārējas žalūzijas, lai novērstu taranēšanu;
- stikls, kas ir izturīgs pret triecienviļņa iedarbību, un fiziska aizsardzība pret nelieliem spridzekļiem;
- cilvēku pārvietošana prom no logiem un monitoru novietošana tā, lai no ārpuses tos nevarētu redzēt.

***RF* uzraudzība**

UAS ekspluatācijai izmanto dažādas sakaru frekvences. *UAS* izmantoto frekvenču joslu nosaka konkrētais pielietojums, *UAS* veids un ekspluatācijas reģions. Kopumā *UAS* sakariem ar zemes kontroles staciju, citiem bezpilota lidaparātiem un satelītsakariem izmanto gan atļautas, gan neatļautas frekvenču joslas.

Tiešā attālā identifikācija[23] ir atvērtā protokola signāls, ko visā lidojumā pārraida reāllaikā. Šo tiešo regulāro apraidi no bezpilota lidaparāta, kas izmanto atvērtu un dokumentētu pārraides protokolu, var saņemt tieši, izmantojot esošās mobilās ierīces, kas atrodas apraides diapazonā. Tajā ir vismaz turpmāk norādītie dati.

- *UAS* ekspluatanta reģistrācijas numurs un reģistrācijas procesā dalībvalsts norādītais verifikācijas kods.
- Unikālais bezpilota lidaparāta sērijas numurs.
- Laika zīmogs, bezpilota lidaparāta ģeogrāfiskā atrašanās vieta un tā augstums virs virsmas vai pacelšanās punkta.
- Azimuts, kas mērīts pulksteņrādītāja kustības virzienā no ģeogrāfiskajiem ziemeļiem, un bezpilota lidaparāta zemes ātrums.
- Pilota ģeogrāfiskā atrašanās vieta vai, ja tā nav zināma, pacelšanās punkts.

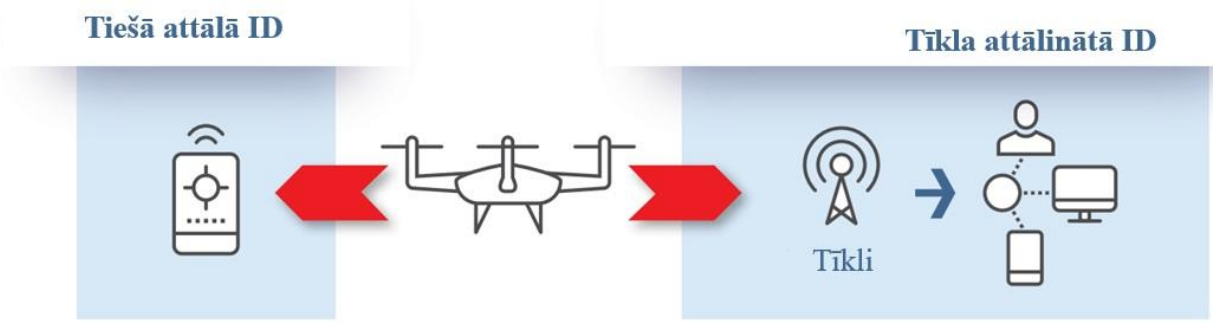
To pašu informāciju var iegūt, izmantojot tīkla attālināto ID. Tiešo attālo ID pārraida tieši no bezpilota lidaparāta uz uztvērēju, toties tīkla attālinātās ID informāciju pārraida no bezpilota lidaparāta uz mobilajiem tīkliem (globālā mobilo sakaru sistēma), kas to izplata tālāk. Šis process ir parādīts 17. attēlā. Risinājumā iekļaujot ārējus pakalpojumus, kuriem ir pieejama

[22] Aizsardzība pret bezpilota lidaparātu sistēmām. Rokasgrāmata par bezpilota lidaparātu sistēmu riska novērtēšanu un ēku un objektu fizisku nostiprināšanu

[23] https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems?page=19.

tīkla attālinātās ID informācija, vēlams iekļaut šo informāciju, taču tā nav uzskatāma par būtisku pasākumu minimumu.

16. attēls. Attālas ID veidi



Lai gan ir svarīgi saņemt *UAS* ID, jāpieņem, ka daudzas *UAS* un jo īpaši nesadarbīgās *UAS* to nepārraidīs. Tāpēc ir arī jānovēro frekvenču joslas, ko visbiežāk izmanto *UAS* sakariem, kā parādīts 18. attēlā.

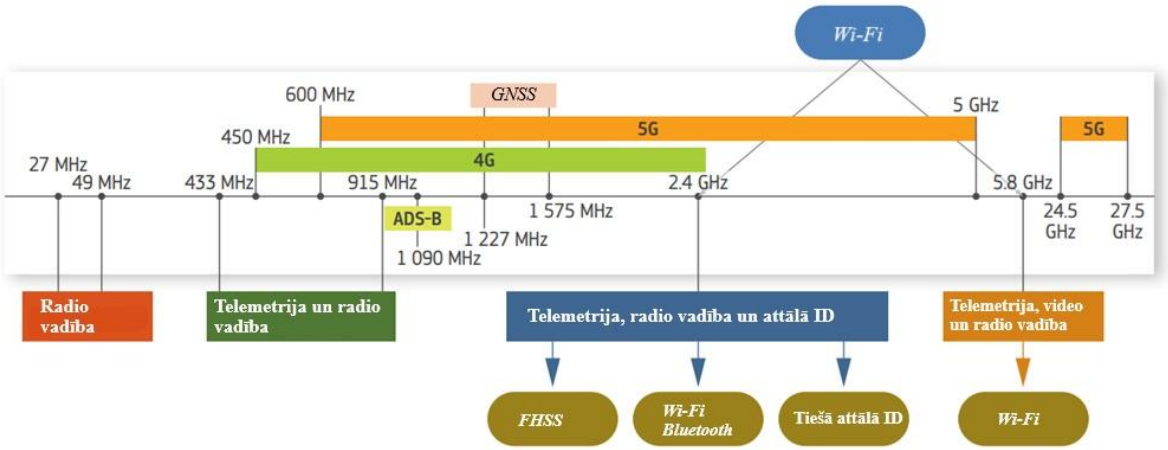
Komerciālu *UAS* diezgan lielā mērā līdzinās *Wi-Fi* maršrutētājam, kas pilotam nosūta video kadrus un lidojuma datus. Vairākums komerciālo *UAS* izmanto 2,4 GHz un 5,8 GHz, kas ir arī parastās *Wi-Fi* savienojuma frekvences. Nosakot un interpretējot *UAS* attālo signālu informāciju, var iegūt vērtīgu papildinformāciju, piemēram, par *UAS* modeli un ražotāju, *GNSS* pozīciju, pacelšanās pozīciju (parasti saistībā ar pilota atrašanās vietu), akumulatora uzlādes līmeni, videspiekļuves vadības adresi, *UAS* vadības komandu veidu un lidojuma režīmiem.

UAS var darboties arī atļautās frekvencēs, piemēram L joslā (1–2 GHz) un S joslā (2–4 GHz), ko parasti izmanto satelītsakariem. Minētās frekvences nodrošina stabilu un drošu saziņu lielos attālumos, tāpēc tās ir piemērotas ekspluatācijai ārpus tiešās redzamības. Papildus minētajām joslām *UAS* izmanto arī citas frekvenču joslas, piemēram, satelītsakariem C joslu (4–8 GHz) un Ku joslu (12–18 GHz), bet aizsardzības pielietojumiem – ultraīsviļņu frekvenču joslu (300–400 MHz).

Noteiktu frekvenču joslu izmantošanai, iespējams, ir nepieciešama atļauja, un dažādām valstīm attiecībā uz *UAS* sakaru frekvencēm var būt atšķirīgi noteikumi. Tādēļ, lai nodrošinātu atbilstību attiecīgās valsts normatīvajiem aktiem, ir svarīgi pārzināt ekspluatācijas reģiona tiesisko regulējumu.

Lai gan tā tiek uzskatīta par vienkārši uzstādāmu tehnoloģiju (pasīvā *RF* antena), tās darbība ir tieši saistīta ar uzstādīšanas vidi, piemēram, attālumu līdz ēkām un kokiem. Turklāt *RF* tehnoloģijas uztveršanas diapazonu ietekmē uztvērēja jutīgums un *UAS* raidītāja *RF* signāla jauda.

17. attēls. UAS izmantotās frekvences



Mijiedarbība ar ieinteresētajām personām

Tā kā, iekļaujot ieinteresētās personas procesos un procedūrās, tās palīdz nodrošināt efektīvu un lietderīgu ieviešanu, mijiedarbība ar ieinteresētajām personām ir viens no būtisku pasākumu minimuma pasākumiem, kas jāveic jebkurā risinājuma projektā. Visos *C-UAS* risinājuma posmos būs iesaistītas dažādas ieinteresētās personas. Konkrētas ieinteresētās personas, kas jāiesaista *C-UAS* risinājumā, katrā objektā un katram pieņemtajam eskalācijas līmenim būs atšķirīgas. Ieinteresētajām personām ir jāvienojas par to, kurš ko, kur un kad darīs.

Kiberdrošība

Visiem ieviestajiem risinājumiem, kuros izmanto IKT, obligāti ir jāveic IKT drošības nostiprināšana. Tā kā *C-UAS* sistēmas ir drošības informācijas sistēmas un tās paredzēts iekļaut citās drošības sistēmās, visus tīkla pieslēgumus ir iespējams izmantot, lai ielauztos un pārveidotu konfigurācijas vai sagrautu sistēmas. Ja *C-UAS* risinājums ir pieslēgts internetam, ir rūpīgi jāanalizē šo pieslēgumu drošības riski. Pilnīgais risinājums ir jāiekļauj objekta uzņēmējdarbības nepārtrauktības plānā, kiberdrošības politikā, drošības procedūrās un pieņemamā riska līmenī.

3.2. MAZINĀŠANAS LĪMEŅA IZVĒLE UN IDENTIFICĒŠANAS TEHNOLOĢIJU PIELĀGOŠANA

C-UAS risinājuma projektā izvēlas piemērotu reakciju uz KI objekta vai sabiedriskas vietas apdraudējumu un pēc tam to salāgo ar atbilstīgiem pasākumiem. Ņemot vērā šo pasākumu iespējamo ietekmi uz paredzētajiem mērķiem, to darbības vidi un nodomu šīs ierīces izmantot civilā vidē, pirms lēmuma par to pieņemšanu ir jānosaka šo pasākumu likumīgums. Katrā dalībvalstī attiecībā uz tehnoloģiju izmantošanu var būt atšķirīgi tiesību akti. Katram KI objektam vai sabiedriskai vietai ir ieteicams savās valsts un vietējās iestādēs noskaidrot piemērojamos noteikumus.

Sākotnējais objekta novērtējums un apsekojums palīdzēs noteikt konkrētajām vajadzībām piemērotāko tehnoloģiju. Jāizmanto sākotnējā modelēšana un, veicot objekta apsekojumu, tā jāpamato ar testiem.

14. attēlā ir parādīta mazināšanas līmeņu un tehnoloģiju savstarpējā saikne. Risinājuma izstrādes gaitā vairākas reizes ir jāatkārto mazināšanas līmeņa definēšanas process, tehnoloģiju atlase un ieinteresēto personu iesaistīšana. Neatkarīgi no reakcijas uz apdraudējumu būs vairāki pamatpasākumi, kas jāievieš KI vai sabiedriskajai vietai.

Šajā metodikā ņem vērā uzraudzību, pasīvus mazināšanas pasākumus un aktīvus mazināšanas pasākumus, tos skaidri nenodalot, skat. 19. attēlu. Tie papildina pamatpasākumu sniegtās priekšrocības.

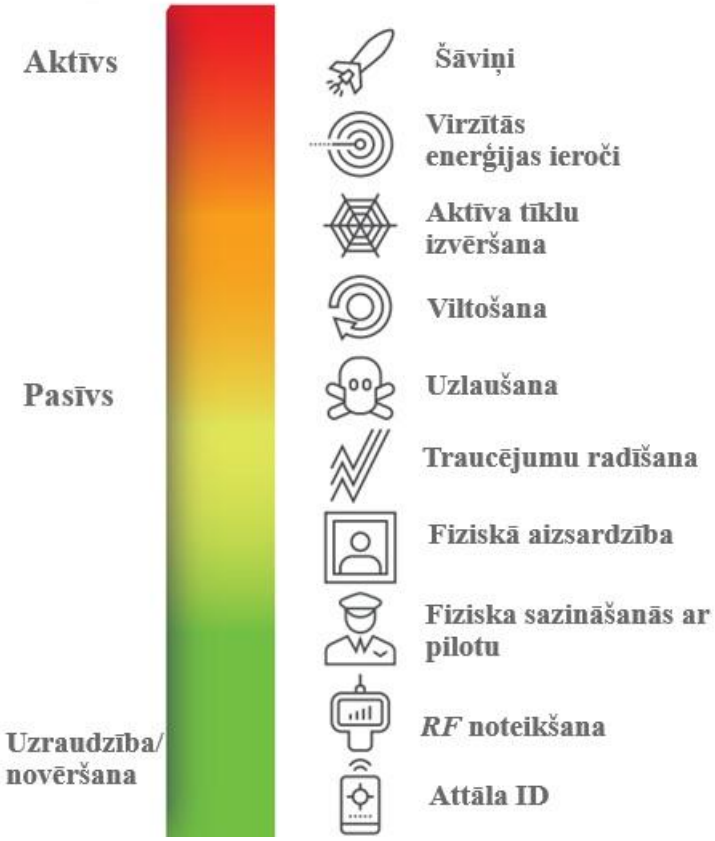
Uzraudzība/novēršana ir zemākais apdraudējuma mazināšanas līmenis. Šajā apdraudējuma novēršanas līmenī notiek *UAS* satiksmes atklāšana un novērošana noteiktajās zonās un vēršanās pie *UAS* pilotiem. Saskaņoto robežu vai noteikumu pārkāpumu gadījumā tas ietver darbības, kas nav saistītas ar iejaukšanos. Šā zemākā aizsardzības līmeņa mērķis ir izprast *UAS* izmantošanu, identificējot *UAS* satiksmi aizsargājamā teritorijā vai objektā.

Pasīvas mazināšanas mērķis ir apturēt notiekošo, izmantojot salīdzinoši nekaitīgus pasākumus, kas varētu ietvert sazināšanos ar pilotu(-iem) un nekinētisku pasākumu izmantošanu.

Aktīva mazināšana ir augstākais no trim minētajiem līmeņiem. Šajā līmenī izmantos visus pieejamos pasākumus, lai apturētu *UAS* apdraudējumu noteiktajā zonā, radot minimālus netiešos bojājumus. To varētu panākt, apvienojot tādus pasākumus kā sazināšanās ar pilotu(-iem), kinētisku un nekinētisku pasākumu izmantošana. Visas procedūras būs pienācīgi jāievieš, saņemot iestāžu atļauju. Mazināšanas dalībnieki varētu būt gan iekšējie, gan ārējie drošības dienesti, piemēram, *LEA* vai aizsardzības nozare.

Lai uzlabotu reaģētspēju, visi pasākumi un darbības būs jāreģistrē.

19. attēls. Mazināšanas līmeņi



Svarīgi, lai apdraudējuma mazināšanas process un ar to saistītās procedūras būtu pienācīgi definēti. To vēlāk izmantos gūtās pieredzes izzināšanai un salīdzināšanai ar citiem risinājumiem. Varētu būt lietderīgi izmantot metodiku, kas ir atzīta un ko izmanto arī līdzīgu tuvumā esošu ieviesto risinājumu ieinteresētās personas, kuras, apmainoties ar informāciju, palīdzēs novērst pārpratumus un neskaidrības Jāuzsver, ka starp riska mazināšanas līmeni un izmantošanai paredzēto tehnoloģiju nav tiešas saistības. Robežvērtības, kas riska skaitliskos novērtējumus sasaista ar eskalācijas līmeņiem, jānosaka katram risinājumam atsevišķi.

Tās jāpapildina ar projekta papildu apsvērumiem, kas saistīti ar *UAS* riska mazināšanu. Vairākumā gadījumu mazināšanas pasākumi būs vai nu kinētiski, vai nekinētiski. Kinētiskie pasākumi ietver fiziska spēka izmantošanu, lai atspējotu vai iznīcinātu *UAS*, taču nekinētiskie pasākumi ietver elektronisku vai citu līdzekļu izmantošanu, lai traucētu *UAS* vai to atspējotu. Pasākumu izvēli noteiks konkrētais apdraudējums, ko rada *UAS* un ekspluatācijas vide, kurā *C-UAS* sistēma tiks izmantota. Šo mazināšanas pasākumu piemērošana un iespējamā vadība jānosaka un jāievieš saskaņā ar valsts un reģionālajām tiesību normām.

Turpmāk aprakstīti visbiežāk izmantotie[24] un pieejamie pasākumi.

[24] https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

Kinētiskie pasākumi ietver fiziska spēka izmantošanu, lai atspējotu vai iznīcinātu *UAS*. Šādi pasākumi var būt tostarp turpmāk minētie.

- **Virzītās enerģijas ieroči** (*DEW*) izmanto augstas enerģijas starus, piemēram, lāzerus vai mikroviļņus, lai atspējotu vai iznīcinātu *UAS*. Kopumā *DEW* nav letāli, taču tomēr var sabojāt *UAS* komponentus.
- **Šāviņi vai raķetes** pretdronu raķetēs izmanto sprāgstvielas vai citus līdzekļus, lai fiziski iznīcinātu *UAS*. Šādas raķetes var būt gan vadītas, gan nevadītas, un tās var palaist no dažādām platformām, tostarp uz zemes bāzētām starta iekārtām vai gaisa platformām.
- **Kājinieku ieročus**, piemēram, šautenes vai bises, var izmantot, lai notriektu *UAS*. Tomēr šī pieeja var būt sarežģīta vai bīstama, jo jāspēj precīzi mērķēt, un tā var radīt nevēlamus bojājumus citiem objektiem vai tos iznīcināt.
- **Tīklu izvēršana** ietver īpaša aprīkojuma izmantošanu, lai gaisā notvertu un apturētu *UAS*, novēršot tās tālāku lidojumu.

Nekinētiskie pasākumi savukārt ietver elektronisku vai citu līdzekļu izmantošanu, lai traucētu vai atspējotu *UAS* darbību. Tie var būt kādi no turpmāk minētajiem pasākumiem.

- ***RF* traucējumu radīšanu** var izmantot, lai traucētu sakarus starp *UAS* un tās pilotu, izraisot *UAS* vadības zudumu un, iespējams, avāriju[25].
- **Viltošana** ir viltus signālu radīšana, lai apmānītu *UAS*, liekot uzskatīt, ka tā saņem īstas sava pilota komandas. Tādējādi *UAS* var piespiest mainīt kursu vai atgriezties izlidošanas vietā.
- **Uzlaušana** ir nesankcionēta iekļūšana *UAS* vadības sistēmā, lai pārņemtu tās vadību vai traucētu darbību.

Izstrādājot *C-UAS* risinājumu, kurā ņem vērā mazināšanas līmeni, jāapsver vairāki faktori, lai nodrošinātu, ka ir izvēlēti piemēroti pasākumi, ar kuriem efektīvi apkarot konkrēto apdraudējumu, ko rada *UAS*, skat. 14. attēlu. Tie ir jāņem vērā papildus pamatpasākumu minimumam, kas jāievieš vienmēr.

Turpmāk uzskaitīti daži svarīgi faktori, kas jāapsver.

- Apdraudējuma novērtējums. Ir svarīgi pastāvīgi novērtēt konkrēto apdraudējumu, ko rada *UAS*. Tas ietver izpratni par *UAS* iespējām, lidojuma parametriem, lietderīgo kravu, kā arī par iespējamajiem mērķiem un paredzēto uzbrukuma ietekmi.
- Jāņem vērā arī ekspluatācijas vide, kurā tiks izmantoti *C-UAS* pasākumi. Daži faktori (piemēram, laika apstākļi, apvidus, lauku vai pilsētas teritorija, troksnis, sensoru uzstādīšanas vietas, tādi šķēršļi kā augstceltnes) ietekmēs *C-UAS* sistēmas veiktspēju. Piemēram, risinājums, ko izmanto uzstādīšanai tuksnesī, atšķirsies no risinājuma, ko izmanto aizsardzībai pilsētā, Ziemassvētku tirdziņā, ūdens attīrīšanas iekārtā vai cietumā.
- Piemēram, **zonas** un to lielums ir jebkura zonu daļa, kura ir kopīga ar citām aizsargātajām zonām.
- Ieviestie **fiziskās aizsardzības** pasākumi vai to ieviešanas plāni.

[25] Tā kā pieejamās ierīces ir izgatavotas, lai traucētu apstiprinātās *UAS* sakaru frekvences, tās nebūs efektīvas pret *UAS*, kuru frekvences ir pārveidotas (skat. 3.1. iedaļu).


NO DRONES

- *UAS* satiksmes informācija, kas saņemta no **identifikācijas sistēmām**, un **pieejamie dati**, kas saņemti no citiem avotiem, piemēram, gaisa telpas pārvaldības iniciatīvām (*UTM* un *U-Space*).
- Pieejamie **dalībnieki un ieinteresētās personas**, kas pilnvarotas izmantot mazināšanas pasākumus. Vai tie ir pieejami tūlīt vai ar tiem ir jāsazinās? Piemēram, *LEA* vai aizsardzības sektors.
- Nepieciešamais laiks, lai visbeidzot rīkotos, iespējams, ir vissvarīgākais faktors.
- Jāapsver *C-UAS* pasākumu **izmaksas**. Tas ietver pašu pasākumu izmaksas, kā arī personāla mācības un iekārtu uzturēšanas izmaksas.
- **Traucējumus un kļūdaini pozitīvus rezultātus** var samazināt, pievienojot papildu sensorus vai izmantojot vairāku veidu sensorus, kā arī apvienojot datus, lai labāk izprastu situāciju. Tomēr tas radīs izmaksas.
- **Juridiski un ētiski apsvērumi.** *C-UAS* pasākumu izmantošana var izvirzīt juridiskus un ētiskus apsvērumus. Noteikti ir jānodrošina, lai visi izvēlētie pasākumi atbilstu attiecīgajiem normatīvajiem aktiem un neapdraudētu neiesaistītās puses.

Rūpīgi apsverot šos faktorus, var izvēlēties piemērotu mazināšanas līmeni. Lai nodrošinātu risinājuma atjaunināšanu atbilstīgi esošajam apdraudējumam un atjauninātajām tehnoloģiju specifikācijām, visi šie faktori ir regulāri jāpārskata, skat. 14. attēlu.

C-UAS sistēmās izmanto ļoti daudzas identificēšanas un izsekošanas tehnoloģijas, un tās strauji attīstās. Turpmāk aplūkotas visbiežāk izmantotās tehnoloģijas.

- **Radiolokators** ir elektroniska ierīce, kas izmanto radioviļņus, lai atklātu objektus un noteiktu to atrašanās vietu. Tas izstaro radioviļņus, kas atstarojas no ceļā sastaptiem objektiem, un radiolokatora sistēma pēc tam identificē atstarotos viļņus, lai noteiktu objekta atrašanās vietu, ātrumu un citas īpašības. Radiolokatorus var izmantot, lai lielā augstumā un lielos attālumos identificētu bezpilota lidaparātus. Tomēr radiolokatora viļņi nevar izkļūt cauri tādiem šķēršļiem kā ēkas vai koki un var nespēt tikpat efektīvi identificēt mazākus bezpilota lidaparātus zemākā augstumā vai pilsētā, kur ir daudz traucējumu.
- ***RF* analīze** identificē *RF* signālus, ko izstaro bezpilota lidaparātu vadības sistēma. Tā kā *UAS* izmanto radio signālus, lai sazinātos ar attālām vadības ierīcēm, *RF* sensori var identificēt signālus, ko izstaro bezpilota lidaparāts un tā vadības ierīce. RF var izmantot mazāku *UAS* identificēšanai zemākā augstumā. Tomēr tie nevar tikpat efektīvi identificēt *UAS*, kas izmanto frekvenču lēcienus vai citus paņēmienus, kas sarežģī noteikšanu.
- **Akustiskie sensori** nosaka skaņu, ko rada bezpilota lidaparātu rotori. Lidojumā *UAS* raida īpašu akustisko atstaroto signālu, kuru var uztvert akustiskie sensori. Akustiskos sensorus var izmantot, lai identificētu zemu lidojošas *UAS*, un tos var izmantot pilsētās, kur citas tehnoloģijas var nebūt tik efektīvas. Tomēr akustiskie sensori var pietiekami labi neatklāt bezpilota lidaparātus, kuriem ir klusāki rotori vai kuri lido trokšņainā vidē.
- **Elektrooptiskie/infrasarkanie (*EO/IR*) sensori** izmanto vizuālu un termisku attēlveidošanu, lai identificētu un izsekotu *UAS*. Šie sensori var noteikt siltumu, ko rada bezpilota lidaparātu motori, vai paša bezpilota lidaparāta vizuālo atstaroto signālu. *EO/IR* sensori var atklāt bezpilota lidaparātus slikta apgaismojuma apstākļos un var efektīvi noteikt *UAS* veidu. Tomēr tie nespēj pietiekami labi atklāt bezpilota lidaparātus lielā attālumā vai apstākļos, kuros bezpilota lidaparāta atstarotais siltuma signālu noslēpj citi vides faktori.

Sensoru apvienošanas programmatūru izmanto, lai apvienotu dažādu sensoru signālus. To var izmantot, lai papildinātu sensoru signālus un apvienotu tos vienotā kopumā. Tas nodrošinās labāku identificēšanas aptvērumu un to, ka tiek izmantotas visu pieejamo identificēšanas tehnoloģiju labākās daļas. Piemēram, sensoru apvienošanas programmatūra var izmantot datorredzi un mašīnmācīšanās algoritmus, lai atklātu *UAS*, analizējot videoinformāciju no videokamerām un apvienojot to ar radiolokatora informāciju. Tā būs iespējams atklāt un izsekot *UAS* reāllaikā un uzlabot lielu teritoriju novērošanu.

Lai gan iepriekš minētās tehnoloģijas spēj efektīvi atklāt un izsekot *UAS*, ir rūpīgi jāapsver *UAS* identificēšanas tehnoloģijas vai tehnoloģiju kombinācijas izvēle. Šos mainīgos ietekmē tas, pret kādām *UAS* objektu mēģina aizsargāt. Šeit jāatceras apdraudējuma novērtējums, kas aprakstīts iepriekšējā riska un apdraudējuma analīzes posmā. Jāpārbauda arī tas, vai tehnoloģijas ir piemērotas attiecīgajam objektam un vai ir nepieciešami pasīvie *RF* sensori vai aktīvā radiolokācijas tehnoloģija, ja tā ir atļauta. Tā kā uz aktīvo pasākumu izmantošanu attiecas vairāk noteikumu, tos bieži vien ir sarežģītāk ieviest (piemēram, spektra atļaujas un jaudas ierobežojumi attiecībā uz radiolokatora izmantošanu).

Turpmāk uzskaitīti svarīgi elementi, kas jāņem vērā, izstrādājot risinājuma tehnisko daļu.

- **Diapazons.** Dažām tehnoloģijām ir plašāks diapazons, un tās var atklāt *UAS* no lielāka attāluma, toties citām tehnoloģijām var būt mazs darbības attālums, un tās var nespēt efektīvi atklāt *UAS*, kas atrodas lielākā attālumā.
- **Vide.** Vide, kurā ir izvietota *UAS* identifikācijas sistēma, var būtiski ietekmēt tehnoloģijas efektivitāti. Piemēram, radiolokators var nespēt efektīvi identificēt *UAS* pilsētās, kur ir daudz traucējumu, vai vietās, kurās ir augstceltnes vai koki, kas var traucēt radiolokatora signālu.
- **Izmaksas.** Svarīgs apsvērums ir arī tehnoloģijas izmaksas. Dažu tehnoloģiju, piemēram, radiolokatoru, uzstādīšana un uzturēšana var būt dārga, toties citas, piemēram, *RF* sensori vai akustiskie sensori, var būt izmaksu ziņā efektīvākas.
- **Kļūdaini pozitīvi rezultāti.** *UAS* identifikācijas sistēmām var būt arī kļūdaini pozitīvi rezultāti, kas var mazināt sistēmas efektivitāti. Piemēram, *RF* sensori var identificēt signālus no citām ierīcēm vai avotiem, bet akustiskie sensori var uztvert skaņas no citiem avotiem, piemēram, putniem vai lidaparātiem.
- **Pretpasākumi.** Dažas *UAS* identifikācijas tehnoloģijas var būt jutīgas pret tādiem pretpasākumiem kā signāla traucēšana vai viltošana. Tas var samazināt identifikācijas sistēmas efektivitāti vai to padarīt pilnīgi neefektīvu.

Jāņem vērā daži svarīgi *UAS* faktori, kas uzskaitīti turpmāk.

- ***UAS* lielums.** Arī *UAS* lielums var ietekmēt identifikācijas tehnoloģijas efektivitāti. Dažas tehnoloģijas var būt labāk piemērotas lielāku *UAS* atklāšanai, toties citas spēj labāk atklāt mazākas *UAS*.
- **Ātrums.** Bezpilota lidaparāta ātrums nosaka laiku, kas pieejams reaģēšanai uz apdraudējumu. Tā kā *UAS*, kas lido ar ātrumu 60 km/h, 120 sekundēs var nolidot 2 km, kā parādīts 21. attēlā, šajā 2 minūšu intervālā *C-UAS* risinājumam ir jāatklāj, jāizseko, jāidentificē un jāmazina apdraudējums.
- **Lidojuma veids.** Ja noziedzīga nodarījuma izdarītājs izmanto automatizētu lidojumu, nebūs *RF* signāla, ko atklāt.

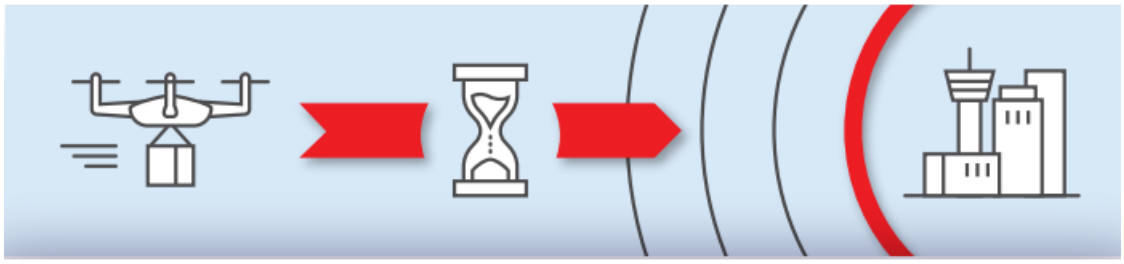
- **Pilota atrašanās vieta.** Ja pilota atrašanās vietas noteikšana ir svarīgs faktors, jāpārdomā turpmāk minētie fakti.
  - Daudzas identifikācijas sistēmas pilota atrašanās vietu nolasa no *UAS* un attālās vadības ierīces sakaru signāliem. Tos var pārveidot vai izslēgt.
  - Attālās vadības ierīces *RF* nosaka, saņemot attālās vadības ierīces raidīto signālu. Vides apstākļu dēļ tas var būt ļoti sarežģīti vai pat neiespējami.
  - Automatizēta lidojuma gadījumā lidojumu nepilotē cilvēks.

Blakus iedarbība

Mazināšanas tehnoloģiju blakus iedarbībai ir svarīga nozīme, un tā ir rūpīgi jāanalizē, jo īpaši, ja vēlāk paredzēti neitralizācijas pasākumi.

- Vadības signālu traucēšana var ietekmēt arī citas iekārtas, kas izmanto to pašu *RF* joslu.
- Viltošana un uzlaušana var ietekmēt *UAS* lidojumu, un tā var avarēt vai ielidot citās zonās, kur varētu radīt bojājumus.
- Šāviņi vai raķetes aizlido garām mērķim un var sabojāt infrastruktūru un ievainot cilvēkus.
- *DEW* var gan sabojāt *UAS*, gan arī ietekmēt citas ierīces.

20. attēls. *UAS* laiks līdz mērķa sasniegšanai



Ar 60 km/h (kategorija 0 maks.) 2 km = 120 sekundes

Jo ilgāks laiks nepieciešams, lai reaģētu un ierobežotu incidentus, jo lielāka būs nepieciešamā paziņošanas zona. Lai nodrošinātu pietiekami daudz laika mazināšanas pasākumu aktivizēšanai, ātrākas *UAS* ir jāatklāj daudz lielākā attālumā.

PADOMS

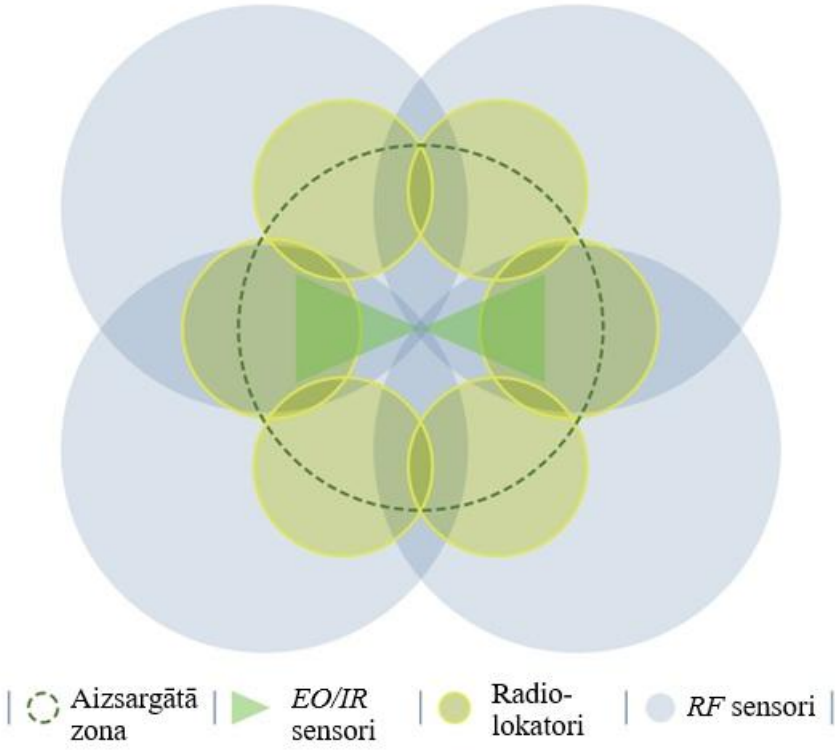
Tiklīdz potenciālais apdraudējums ir atklāts un identificēts, risinājumam ir ātri jāreaģē, lai to mazinātu. To var izdarīt, veicot tādus pretpasākumus kā sazināšanās ar pilotu, sakaru traucēšana vai citi pārtveršanas paņēmieni.

Sensoru izvietojums

Šajā daļā izklāstīts, kā izvietot sensorus, kas izvēlēti *UAS* atklāšanai. Lai nodrošinātu vislabāko atklāšanas pārklājumu, saistībā ar sensoriem jāanalizē ekspluatācijas vide un iespējamais apdraudējums. To var izdarīt, izmantojot modelēšanas un simulācijas rīkus, ko papildina praktiski izmēģinājumi un izvērtējums. Lai nodrošinātu pareizu identifikāciju un izvairītos no aklajām zonām, visi modeļi un simulācijas ir jāpārbauda praksē.

Lai nodrošinātu vairākkārtēju pārklājumu un redundanci (piemēram, "Šveices siera" modelis[26]), jāapsver dauzslāņu drošības sistēmas izveide, izmantojot vairākas identifikācijas sistēmas, piemēram, radiolokatorus, videokameras un akustiskos sensorus.

21. attēls. Piemērs zonas aizsardzībai ar vairākiem atšķirīgiem sensoriem



Ieviešot identifikācijas sistēmas, ir izšķiroši svarīgi ņemt vērā ekspluatācijas vidi. Apvidus, laika apstākļi un iespējamie šķēršļi ļoti ietekmēs risinājuma darbība efektivitāti. Līdztekus risinājumam nepieciešamo identifikācijas sistēmu izvietošanai svarīgi ir vairāki faktori, un tie ir jāņem vērā, lai nodrošinātu optimālu aizsardzības aptvērumu.

Tie var būt, piemēram, turpmāk minētie faktori.

- Izpratne par apdraudējuma scenārijos aprakstīto konkrēto bezpilota lidaparāta radīto apdraudējumu teritorijā, kurā tiks ierīkots *C-UAS* risinājums. Tas nozīmē izprast iespējamo bezpilota lidaparāta veidu, ekspluatācijas augstumu un lidaparāta ātrumu, kā arī iespējamo pārvadāto lietderīgo kravu.

[26] "Šveices siera" nelaimes gadījumu cēloņsakarību modelis uzskatāmi parāda, ka, lai gan starp apdraudējumu un nelaimes gadījumiem ir vairāki aizsardzības slāņi, katrā slānī ir caurumi, kuriem sakrītot, negadījums var notikt.

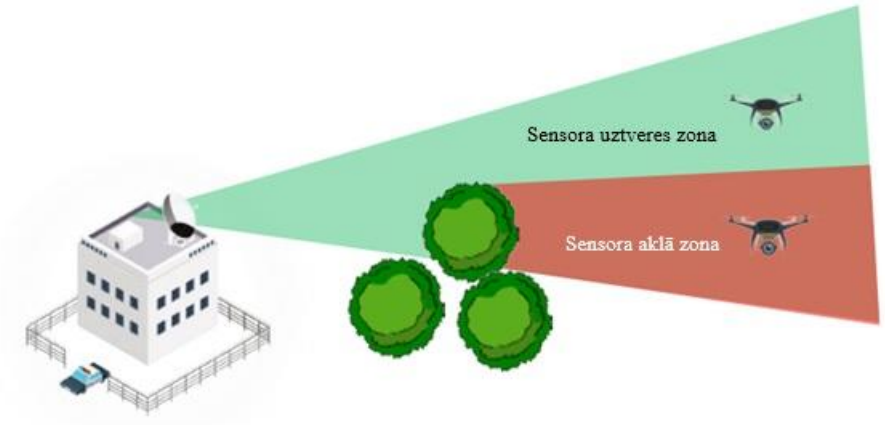
- Lemjot par izvietojumu, jāņem vērā sistēmas uztveršanas diapazons un iespējas. Spēja atklāt dažādus bezpilota lidaparāta veidus, kā arī tās diapazons, precizitāte un reakcijas laiks. Tālas darbības sistēmas un labākas atklāšanas iespējas ļauj precīzāk atklāt *UAS* no lielāka attāluma, tādējādi nodrošinot vairāk laika reaģēšanai.
- Apvidus un šķēršļi, kas atrodas teritorijā, var ietekmēt identifikācijas sistēmu efektivitāti. Piemēram, kā parādīts 23. un 24. attēlā, ēkas, koki un citas konstrukcijas var bloķēt vai atstarot signālus, savukārt pakalni vai kalni var ierobežot tiešās redzamības uztveršanas diapazonu.
- Izvietojums, izvairoties no signāla vājināšanas vai atstarošanas no tādiem avotiem kā ēkas, lapotne vai ūdens.
- Jāņem vērā arī identifikācijas sistēmas ierīkošanas loģistika. Tas ietver elektroenerģijas pieejamību un savienotību ar tīklu, kā arī piekļūstamību teritorijai, kurā paredzēts uzstādīt sistēmu.
- Lemjot par identifikācijas sistēmu izvietošanu, jāņem vērā ekspluatācijas vide, ieskaitot laika apstākļus un iespējamos šķēršļus. Tas ietver iespējamo neaizsargāto zonu apzināšanu un identifikācijas sistēmu izvietošanu stratēģiskās vietās, lai nodrošinātu vislabāko pārklājumu. Lemjot par sensoru uzstādīšanu, būtiska nozīme būs videi un atrašanās vietai.
- Lai palielinātu uztveršanas diapazonu, jāapsver sensoru montēšana uz infrastruktūras, mastiem vai torņiem. Var arī apsvērt iespēju ierīkot dalītu sensoru sistēmu, skat. 24. attēlu.
- Iekļaušana citos *C-UAS* pasākumos. Identifikācijas sistēmu izvietojums ir jāpārdomā arī saistībā ar citiem *C-UAS* pasākumiem, piemēram, kinētiskiem vai nekinētiskiem pasākumiem. Identifikācijas sistēmu izvietošana stratēģiskās atrašanās vietās var uzlabot citu *C-UAS* pasākumu efektivitāti.

Lemjot par sensoru izvietojumu, ir jāpārbauda elektromagnētiskie traucējumi. Tos dēvē arī par *RF* spektra *RF* traucējumiem. Elektromagnētiskie traucējumi ir tādi traucējumi, ko rada kāds ārējs avots, kas ietekmē elektrisko ķēdi, izraisot elektromagnētisko indukciju, elektrostatisko saiti vai elektrovadītspēju. Piemēram, izmantojot radiolokatorus transporta jomā (piemēram, fotoradarus, transporta radaru sistēmas), var radīt traucējumu avotus, kas ietekmē *C-UAS* radiolokatoru sistēmas, vai pretēji, tādējādi ietekmējot sensoru datu kvalitāti un, iespējams, radot kļūdaini pozitīvus rezultātus. Citi iespējamie izraisītāji varētu būt mobilie tālruņi, kosmiskie trokšņi, apgaismojums vai elektrības kabeļi.

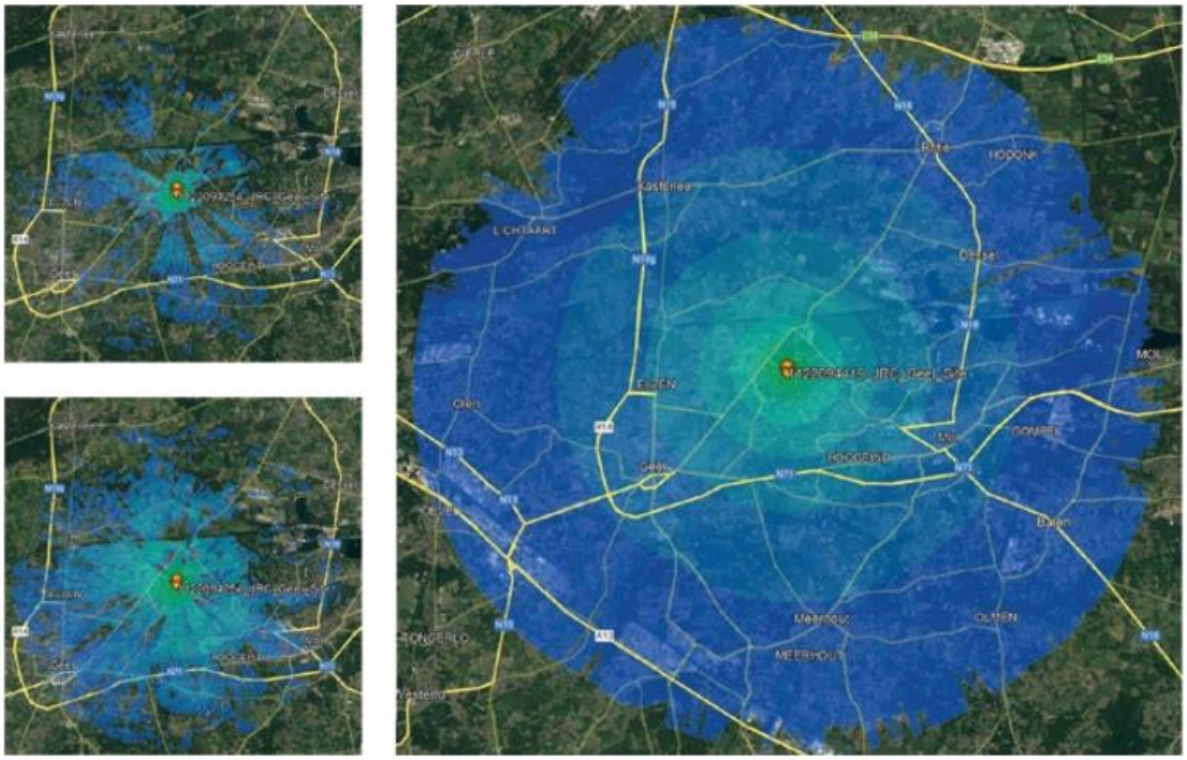
Sensoriem varētu būt nepieciešama redzamības līnija, tāpēc šķēršļi var tieši ietekmēt identificēšanu. Jāņem vērā tādi signāla vājināšanas vai atstarošanas avoti kā konstrukcijas (augstceltņu tuvums, vēja turbīnas, ūdenstorņi un rūpnieciskās iekārtas), meži (teritorijas ar biezu lapotni un potenciālā koku augšana) un ūdens (īpaša uzmanība jāpievērš vietām upju, jūras, ezeru u. c. tuvumā). Turklāt tādas meteoroloģiskas parādības kā migla, lietusgāzes un sniega uzkrāšanās uz sensoriem bieži ietekmē augstfrekvences joslas.

Tādēļ, lemjot par identifikācijas sistēmu izvietošanu, rūpīgi jāpārdomā ekspluatācijas vide, ieskaitot laika apstākļus un iespējamos šķēršļus. Lai nodrošinātu precīzu identifikāciju un mazinātu kļūdaini pozitīvu rezultātu daudzumu, rūpīgi jāizvērtē uztveršanas diapazons, fiziski šķēršļi un elektromagnētiskie traucējumi.

22. attēls. Sensora aklo zonu piemērs (oranžā zona)



23. attēls. Zilajā apgabalā parādīts atklāšanas aptvērums – mainot sensoru izvietojumu, var panākt atšķirīgu pārklājumu.



3.3. RISINĀJUMA ARHITEKTONISKĀ PROJEKTĒŠANA – VISU APVIENOJOT

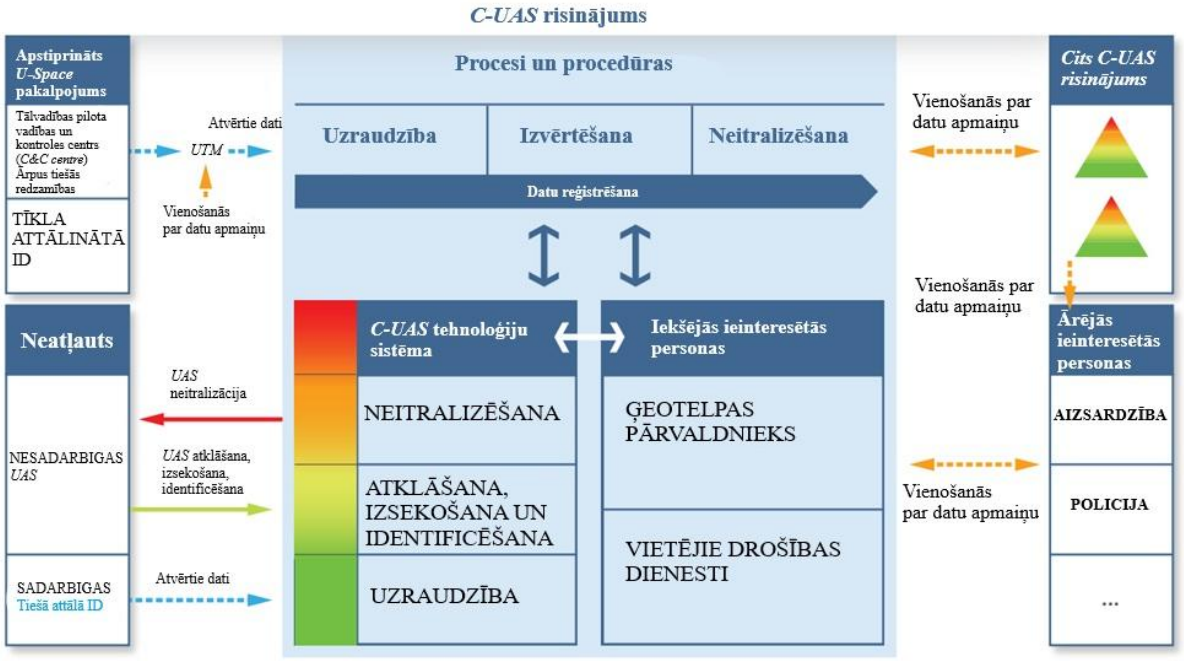
Risinājuma projekts nosaka tā turpmāko spēju paredzētajā darbības laikā saglabāt atbilstību un atjaunināšanas iespējas. Risinājuma arhitektūra ir pamatelements, kas parasti ietver procesu, procedūru, aparatūras, programmatūras un tīkla komponentu kombināciju.

Turpmāk uzskaitīti daži pamatelementi, kurus var iekļaut parastā *C-UAS* risinājumā.

- **Sensori.** Tostarp var būt dažādi sensoru veidi, piemēram, radiolokatori, *EO/IR* un akustiskie sensori, ko izmanto, lai atklātu un izsekotu iespējamo *UAS* apdraudējumu.
- **Sakaru sistēmas un tīkla infrastruktūra.** Tās izmanto, lai sensoru datus pārsūtītu uz centrālo vadības un kontroles (*C2*) centru, kur datus var analizēt un izmantot, lai pieņemtu lēmumus par to, kā reaģēt uz apdraudējumu. *C-UAS* risinājumā var būt virkne tīkla komponentu, tostarp serveri, maršrutētāji un slēdži, ko izmanto, lai pārsūtītu datus starp dažādiem sistēmas komponentiem.
- **Vadības un kontroles centrs un grafiskās lietotāja saskarnes.** Tie ir *C-UAS* risinājuma smadzeņu centrs, kur tiek saņemti, analizēti visi sensoru dati un izmantoti lēmuma pieņemšanai par reaģēšanu uz iespējamo *UAS* apdraudējumu. Vadības un kontroles centrā var būt virkne programmatūras rīku datu analīzei, vizualizācijai un lēmumu pieņemšanai.
- **Izpildmehānismi.** Šos rīkus izmanto *UAS* apdraudējuma mazināšanai. Tās var būt traucēšanas sistēmas, kas rada *UAS* sakaru vai navigācijas sistēmu traucējumus, vai citi rīki, piemēram, lāzeri, ko izmanto, lai atspējotu vai iznīcinātu *UAS*.
- **Lietotāja saskarnes citām ieinteresētajām personām** Šīs saskarnes izmanto ieinteresētās personas mijiedarbībai ar *C-UAS* sistēmu. Tās var ietvert datu vizualizācijai un lēmumu pieņemšanai paredzētas grafiskās lietotāja saskarnes vai speciālas saskarnes informācijas vai datu paziņošanai un *UAS* apdraudējuma mazināšanai izmantoto izpildmehānismu kontrolei.

Kopumā *C-UAS* risinājuma arhitektūra ir projektēta tā, lai atklātu potenciālo apdraudējumu, analizētu datus nolūkā noteikt atbilstīgu reakciju un pēc tam izmantotu izpildmehānismus apdraudējuma neitralizēšanai. Risinājumu arhitektūras specifiskie komponenti atšķirsies atkarībā no attiecīgajām sistēmas prasībām un apdraudējuma veidiem, kuru novēršanai tā ir paredzēta.

24. attēls. Risinājuma arhitektūras piemērs

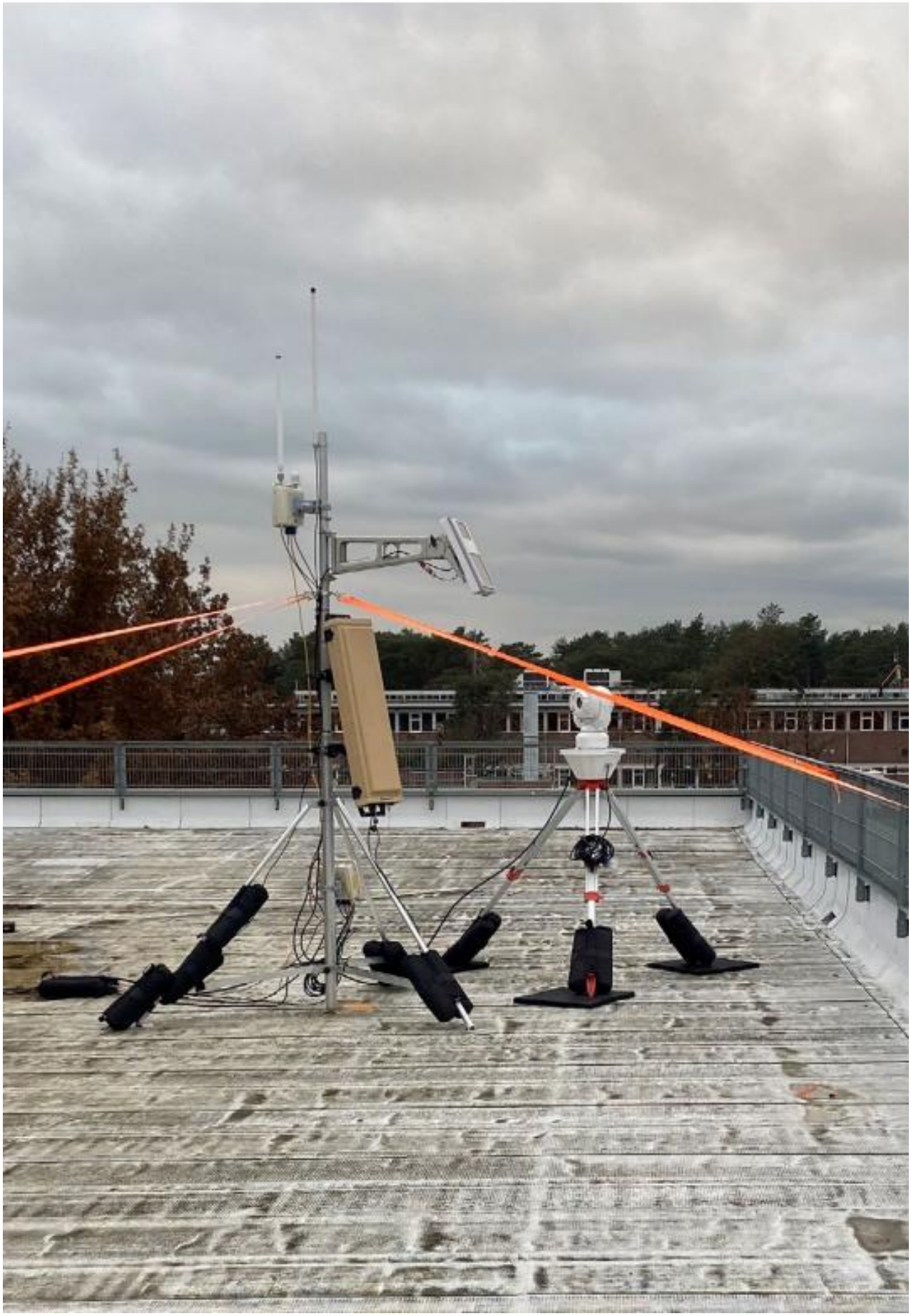


Šajā rokasgrāmatā ieteikts izstrādāt *C-UAS* risinājumu ar atvērtu arhitektūru, kas ļauj iekļaut aparatūru, programmatūru un komponentus, kuri izmanto kopīgus standartus. Tas atvieglos citu uzņēmumu izstrādātu komponentu pievienošanu, nomaiņu un aizvietošanu.

Tā kā tehnoloģijas strauji attīstās un pilnveidojas, *C-UAS* tirgū būs pieejamas jaunas iespējas, un objekta situācijas izmaiņu un no tām izrietošo risku dēļ būs jāpielāgo risinājuma konfigurācija. Tāpēc, ieviešot risinājumu, kura pamatā ir atvērtas arhitektūras pieeja, risinājuma izmaiņas varēs ieviest vieglāk un lētāk.

Dažkārt atvērtu arhitektūras sistēmu projektos iesaka izmantot turpmāk minētos kvalitātes atribūtus.

- **Pielāgojamība.** Piemērojamība dažādu platformu prasībām.
- **Modularitāte.** Komponentiem jābūt neatkarīgi atdalāmiem no sistēmas.
- **Pārnesamība.** Risinājumam jābūt pārnesamam no vienas sistēmas uz citu.
- **Mērogojamība.** Risinājumam jābūt palielināmam vai samazināmam atbilstīgi nepieciešamībai.
- **Sadarbspēja.** Efektīva datu apmaiņa ar citām sistēmām.



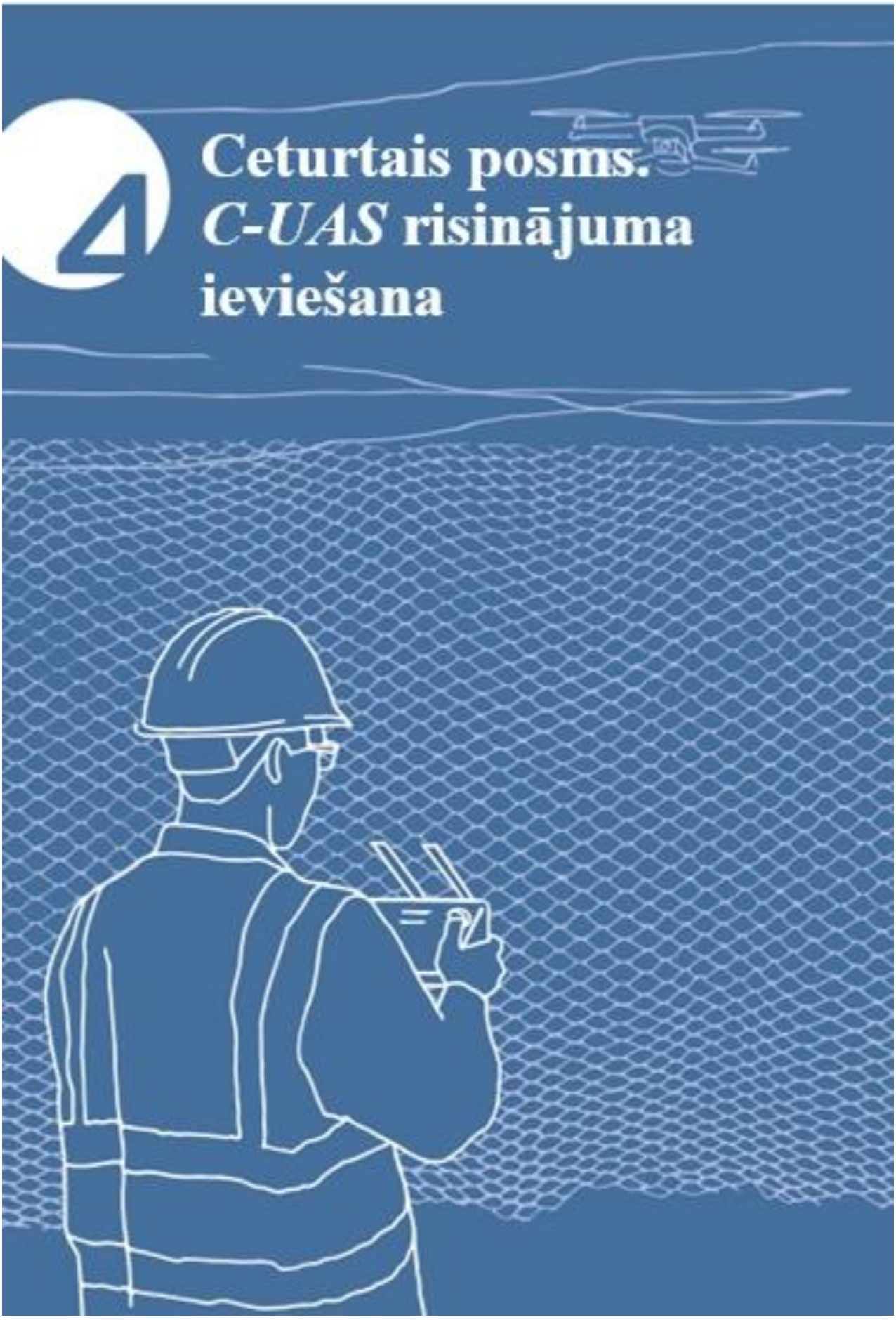
Līdztekus šiem raksturlielumiem projektēšanas lēmumu papildu virzītājspēks būs sistēmas izmaksas. Visbeidzot tā būs pieejamā *C-UAS* budžeta funkcija. Lai nodrošinātu sadarbspēju, šajā rokasgrāmatā ir ieteikts risinājuma izstrādei skatīt vispāratzītus *C-UAS* nozares un arhitektūras standartus un vispārējus protokolus.

8. IZCĒLUMS. PROJEKTĒŠANAS POSMA KOPSAVILKUMS

Projektēšanas posma beigās ir jābūt savāktai informācijai un izstrādātiem plāniem. Tajos būs iekļautas objekta, atrašanās vietas, vides, ieinteresēto personu, noteikumu, (valsts un reģionālo) iestāžu utt. vajadzības.

Šo dokumentu un plānu formāts un detalizācijas pakāpe var atšķirties, un nepieciešamības gadījumā tie ir jāatjaunina. Daži dokumentu piemēri ir:

- objekta risku reģistrs;
- apdraudējuma skaidrojums;
- izpratne par tiesību aktu prasībām;
- atjaunināts objekta apsekojums;
- objektam atbilstīgs risinājuma projekts;
- risinājuma arhitektūra un specifikācijas;
- informācija par objektu un vidi;
- procesi, procedūras un darbības plāni:
- atjaunināta ieinteresēto personu analīze, nosakot konkrētas funkcijas un pienākumus;
- riska un apdraudējuma skaidrojums un apdraudējuma scenāriji, kas jāmazina un pret ko jāaizsargā;
- skaidri noteiktas visu ieinteresēto personu funkcijas un pienākumi;
- augsta līmeņa risinājuma arhitektūra;
- risinājuma prasību specifikācijas.


4
Ceturtais posms.
C-UAS risinājuma
ieviešana

Tiklīdz visas prasības ir skaidri definētas, risinājums izstrādāts, integrators(-i) atlasīts(-i) un formulētas sistēmas specifikācijas, jāizstrādā risinājuma ieviešanas plāns. Tas būs jāizstrādā sadarbībā ar visām ieinteresētajām personām. Atbilstīgi prasībām, iespējams, būs jāizmanto vairāki integratori ar papildinošām iespējām. Piemēram, *UTM* vai *UAS* paredzētas programmatūras nodrošinātājs, kas apstrādā un vizualizē *C-UAS* aparatūras nodrošinātāja ģenerētos datus. Ja tas ir attiecīgā objekta gadījums, ieteicams apsvērt iespēju strādāt ar integratoriem, kam jau ir pastāvīgs partneru kopums. Tas uzlabos risinājuma pilnīgas integrēšanas, testēšanas un pierādīšanas iespējas. Kopīgs darbs ar daudziem piegādātājiem un to darba koordinēšana, lai panāktu kopīgu risinājumu, var būt sarežģīts uzdevums. Ļoti svarīga nozīme ir projekta vadītājam, kuram ir pieredze šajā jomā. Turklāt līgumi ar piegādātājiem ir precīzi jāizstrādā, un tiem jābūt konkrētiem, lai skaidri norādītu visas ieinteresētās personas, pienākumus un jo īpaši saskarnes starp procesiem. Daudzos gadījumos var būt lietderīgi izmantot pakalpojumu modeļus, kuriem ir konkrēti un sīki izstrādāti pakalpojumu līmeņa nolīgumi (*SLA*). Lai sāktu ieviešanu objektā, jābūt gatavām visām ieinteresētajām personām, objektiem un infrastruktūrai. Lai mazinātu problēmas un izvairītos no ilgas kavēšanās, ir svarīgi, lai *C-UAS* risinājumu nodrošinātājs(-i) pēc iespējas ātrāk skaidri izprastu šos īstenošanas priekšnosacījumus. Īstenošanas posmā būs iekļauta uzstādīšanas laika plānošana, testēšanas un kalibrēšanas prasības, operatoru mācības pirms pieņemšanas un nodošana operatīvajiem darbiniekiem. Neizpildot norādītos priekšnosacījumus, var rasties kavējumi, pēdējā brīža pārslodze un budžeta palielinājums.

Šādu priekšnosacījumu piemēri ir:

- tehnoloģiju izmantošanas atļaujas (piemēram, frekvenču izmantošanas atļaujas);
- regulatīvā apstiprināšana;
- speciālas ēkas vai infrastruktūras izmaiņas;
- vides izmaiņas, piemēram, veģetācijas likvidēšana, topoloģijas un objekta apkārtnes izmaiņas;
- infrastruktūras vietas, kurās var uzstādīt sensorus;
- kabeļu sistēma un tīkla infrastruktūra, tostarp tīkla pieslēgums un nepieciešamie telesakari;
- elektrības pieejamība vietās, kurās tiks uzstādīti sensori.

Šajā iedaļā sniegtie padomi jāizmanto kā norādījumi attiecībā uz *C-UAS* risinājuma iekļaušanu objekta parastajā drošības sistēmā un darbībā.


Drone 0.58

9. IZCĒLUMS. CETURTAIS POSMS. RISINĀJUMA IEVIEŠANA

Pirms īstenošanas posma uzsākšanas ir jābūt izpildītiem šādiem punktiem:

- risinājuma projekts;
- objekta apsekojums;
- skaidrs ieviešamā risinājuma prasību apraksts;
- apdraudējuma scenāriji;
- risinājuma un sistēmas specifikācijas;
- arhitektoniskā projektēšana;
- īstenošanas prasības;
- ieinteresēto personu procesi un plāni (kurš ko, kur un kad dara?).

Šā posma beigās jums jābūt izpildītiem šādiem elementiem:

- ieviests organizācijas un riska mazināšanas vajadzībām atbilstīgs risinājums;
- ekspluatācijas rokasgrāmatās ir atjaunināti procesi un procedūras;
- testēšanas un kalibrēšanas ziņojumi;
- risinājuma pārejas plāns;
- atjaunināti ieinteresēto personu saraksti;
- pabeigtas mācības un atjaunināti mācību plāni;
- *C-UAS* risinājums iekļauts parastajā darbībā;
- pilnīga dokumentācija, kas ļauj pāriet no uzstādīšanas uz darbību.

4.1. KALIBRĒŠANA, SISTĒMU UN C-UAS SISTĒMAS VEIKTSPĒJAS VERIFICĒŠANA UN VALIDĀCIJA

Tehniskie un kalibrēšanas testi ir svarīga ieviešanas posma daļa. Šie testi ir jāizstrādā un jāizpilda tā, lai tie parādītu pareizu visa risinājuma darbību. Testus var iedalīt mazākos testos, bet galu galā visiem elementiem ir jābūt testētiem. Jāveic arī galīgais risinājuma tests, kas aptver visas procedūras un procesus kopā ar visām sistēmām.

Testa procedūras un protokoli ir skaidri jādokumentē tā, lai testus ik pēc noteikta laika varētu atkārtot. Ziņojumos jādokumentē rezultāti, visi sensoru dati un mijiedarbība. Bieži vien to dara risinājuma piegādātājs, taču jāapsver iespēja šo testu izstrādē un izpildē iesaistīt neatkarīgu pusi.

Lietderīgi būtu iesaistīt ārējus ekspertus, jo īpaši ielaušanās testos. Ielaušanās testiem jāatspoguļo konkrētā risinājuma identificētie riski, apdraudējuma veidi un scenāriji. Ārējas sarkanās komandas tests varētu nodrošināt plašāku tvērumu.

Visos minētajos testos jāpiedalās visām ieinteresētajām personām, kuras turpmāk būs iesaistītas risinājuma izpildē. Viņu sniegtā informācija un validācija ir būtiska. Testi ir arī lieliska iespēja apmācīt ieinteresētās personas un parādīt risinājumu uzņēmumam.

4.2. IEKĻAUŠANA ESOŠAJOS PROCESOS

Ieviestos risinājumus un sistēmas iekļaujot esošajos procesos (piemēram, drošuma un drošības telpas), iespējams, būs nepieciešami jauni procesi. Tie var būt dažādi atkarībā no noteiktā līmeņa reaģēšanai uz apdraudējumu un no attiecīgo tehnoloģiju izvēles. Savlaicīgi jāveic ietekmes un iekļaušanas analīze, lai nodrošinātu vienmērīgu pāreju uz darbībām, jo īpaši, ja šo procesu izmaiņām nepieciešamas iekšējas vai ārējas atļaujas. Galvenie šīs analīzes rezultāti jāatspoguļo pārejas, mācību, darbības un uzturēšanas plānos.

4.3. OPERATORU UN IEINTERESĒTO PERSONU IZGLĪTOŠANA UN MĀCĪBAS

Ieviešot jaunus procesus vai tos atjauninot, papildu sistēmas un procesus, darbības veidus un darbības izmaiņas, būs jānodrošina mācības jauniem darbiniekiem un ieinteresētajām personām vai jāveic pārkvalifikācija. Attiecīgi ir jāmāca lietot jaunas cilvēka-mašīnas saskarnes, uzraudzības rīkus vai izmantot un uzturēt aparatūru.

Ieteicama rūpīga analīze un mācību plāni. Tajos jāņem vērā tādi noteicošie faktori kā darbinieku pieejamība un mācību atkārtošanās. Lai sagatavotu darbiniekus, kuri ir svarīgi uzdevuma izpildei, parasti pirms tam ilgāk jāplāno resursi, un spēju plānošana ir sarežģītāka. Mācību plānu izstrāde, visticamāk, būs sākusies jau izstrādes posmā.

Lai nodrošinātu optimālu risinājuma darbību, ieinteresēto personu mācībām par *C-UAS* risinājumu jābūt prioritātei. Mācībās jāiekļauj noteikumu (ES un valsts) interpretācija un piemērošana.

Tā kā darbības vieta var pārmaiņus būt gan objekta robežās, gan zonā ap objektu, tas ir jāņem vērā mācībās. Šajās zonās būs atšķirīgi noteikumi un procedūras, un mācības palīdzēs komandām nodrošināt optimālu risinājuma darbību. Ja iespējams, varētu būt lietderīgi mācībās iesaistīt vietējās iestādes, *LEA*, blakus esošos objektus, lidostas, lidlaukus un *UAS* klubus. Tā varētu izmēģināt vairāk *C-UAS* vērtību ķēdes elementu.

4.4. PIEŅEMŠANA UN NODOŠANA EKSPLUATĀCIJĀ

Projekta pieņemšana un nodošana darbības režīmā ir process, kurā projekta grupa pabeigto projektu nodod ekspluatācijas komandai, kas atbildēs par risinājuma uzturēšanu, ekspluatāciju un objekta aizsardzību, izmantojot risinājumu. Nodošanas process ir ļoti svarīgs posms, ar ko nodrošina, ka projekta mērķi ir sasniegti un galīgā aizsardzība ir nodrošināta atbilstīgi riska, projekta un darbības vajadzībām. Pabeidzot uzstādīšanu, testēšanu un mācības, risinājums jānodod darbības nodrošināšanas komandai. Šim svarīgajam posmam bieži vien nepievērš pietiekamu uzmanību un nenovērtē, tāpēc nodošana notiek neatbilstīgi un īstenošanas posms pakāpeniski beidzas ar ražošanu. Šādi var pietrūkt izpratnes par funkcijām un pienākumiem, tādējādi ļoti pasliktinot kopējo risinājuma efektivitāti.

Tāpēc, pieņemot projektu un nododot to ekspluatācijā, jāveic turpmāk minētās darbības.

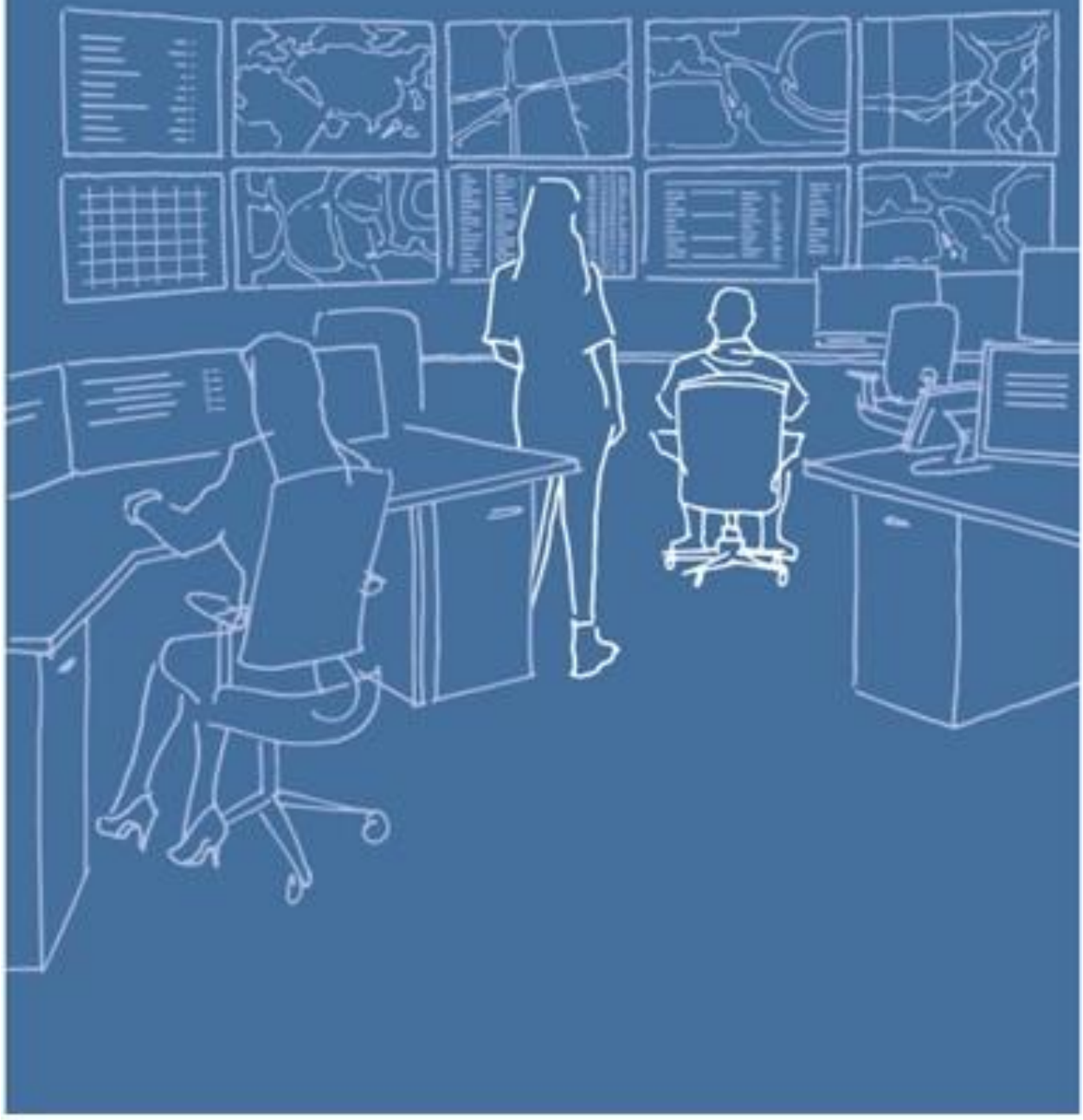
- Projekta grupai jāveic projekta galīgā izvērtēšana, lai nodrošinātu, ka tas atbilst noteiktajām risinājuma prasībām, tam nav nepilnību un kas atbilst kvalitātes standartiem.
- Projekta grupai jādokumentē risinājums, iekļaujot visus attiecīgos dokumentus, piemēram, projekta dokumentus, testu rezultātus un plānus. Šo dokumentāciju darbības nodrošināšanas komanda izmantos atsaucei.
- Lai pārrunātu nodošanas procesus un prasības, jārīko sanāksmes par nodošanu ekspluatācijā, piedaloties risinājuma ieviešanas grupai, darbības nodrošināšanas komandai un uzņēmuma īpašniekam.
- Skaidri nosaka katra nodošanas procesā iesaistītā komandas locekļa funkcijas un pienākumus. Tas nodrošinās, ka ikviens ir informēts par saviem pienākumiem un var tos efektīvi izpildīt.
- Ieviešanas grupai jānodod visas zināšanas un pieredze darbības nodrošināšanas komandai, lai tā varētu efektīvi uzturēt un izmantot risinājumu.
- Jādokumentē testu un ielaušanās testa rezultāti.
- Visas piekļuves sistēmām (IKT, paroles, piekļuves tiesības u. c.) ir jāpārskata un jāmaina atbilstīgi vietējai drošības politikai un procedūrām.
- Jāsagatavo precīza nodošanas dokumentācija un ieviesēja un uzņēmuma īpašnieka vienošanās.

10. IZCĒLUMS. IEVIEŠANAS POSMA KOPSAVILKUMS

Šā posma beigās jums jābūt pabeigtai risinājuma ieviešanai atbilstīgi projekta dokumentiem un jābūt pabeigtām šādām darbībām:

- organizācijas un riska mazināšanas vajadzībām atbilstīga risinājuma ieviešana;
- procesu un procedūru atjaunināšana ekspluatācijas rokasgrāmatās;
- testēšana un kalibrēšana ar ziņojumiem;
- mācības un atjaunināti mācību plāni;
- ieinteresēto personu sarakstu atjauninājumi;
- *C-UAS* risinājuma iekļaušana parastajā darbībā;
- risinājuma pārejas dokumentācija, kas ļauj pāriet no uzstādīšanas uz darbību;
- uzstādīšana un nodošana uzņēmuma īpašniekam.

5 Piektais posms. *C-UAS* risinājuma izmantošana



Pēc sekmīgas riska analīzes, projektēšanas un ieviešanas risinājums pāriet darbības režīmā. Risinājums ir jāiekļauj darba gaitā un jāvada komandai, kas atbild par objekta drošību. Procedūrās iekļauj visu informāciju, kas nepieciešama, lai mazinātu riskus, pret kuriem ir izstrādāts aizsardzības risinājums. Tā kā risinājuma sarežģītība un iekļaušana daudzviet būs atšķirīga, visi risinājumi, visticamāk, būs atšķirīgi.

Šajā rokasgrāmatas pēdējā iedaļā aplūkoti papildu faktori, kas jāņem vērā, nodrošinot *C-UAS* risinājuma darbību. Šajā posmā C-UAS risinājumam jābūt iekļautam parastajos drošības procesos, un tas jāvada, ievērojot tā objekta noteikumus un tiesību normas, kurā tas ir ieviests.

11. IZCĒLUMS. PIEKTAIS POSMS – RISINĀJUMA DARBĪBA

Šajā posmā nepieciešamā informācija:
- ekspluatācijas rokasgrāmatas un procedūras;
- profesionāli sagatavoti un zinoši operatori, kas pārzina noteikumus un procedūras;
- testēšana un verifikācija, kas apliecina, ka risinājums darbojas atbilstīgi prasībām;
- uzraudzība un galveno darbības rādītāju (*KPI*) pielāgošana un izpildāmā PLV.

Risinājuma darbības procesā ir jāreģistrē norādītie elementi, lai tos vēlāk varētu izmantot pastāvīgiem risinājuma atjauninājumiem:
- incidentu reģistrācija (manuāla un automātiska sistēmas reģistrācija);
- gūtā pieredze un problēmu saraksts;
- incidentu ziņojumi;
- atgriezeniskā saite no tiesībaizsardzības iestādēm un ārējām ieinteresētajām personām.

5.1. IEINTERESĒTO PERSONU PASTĀVĪGA IESAISTE UN INFORMĒŠANA

Lai nodrošinātu jebkuras darbības panākumus, izšķiroša nozīme ir ieinteresēto personu pastāvīgai iesaistei un informēšanai. Drošības apsvērumu dēļ dažkārt tas var būt sarežģīti, un ir jādalās tikai ar tādu informāciju, kas ir nepieciešama, neapdraudot vispārējo drošību. Turpmāk izklāstīti daži apsvērumi par to, kā pastāvīgi iesaistīt un informēt ieinteresētās personas.

- Skaidri apziniet ieinteresētās personas, to intereses un tām sniedzamo informāciju. Tas palīdzēs pielāgot informācijas un iesaistes darbības atbilstīgi viņu vajadzībām. Tās ir gan iekšējās ieinteresētās personas (darbinieki, vadība), gan ārējās ieinteresētās personas (*LEA*, klienti, pārdevēji, partneri).
- Izstrādājiet saziņas plānu, kurā izklāstīts, kā sazināsities ar savām ieinteresētajām personām, kādu informāciju jūs varat, un vēlaties sniegt un cik bieži to darīsiet. Rūpīgi analizējiet, kurus kanālus izmantot (e-pasta ziņojumi, sociālie mediji, informatīvi paziņojumi un sanāksmes ir vislabākie kanāli saziņai ar ieinteresētajām personām).
- Regulāri sniedziet jaunāko informāciju par projekta virzību un jebkādām izmaiņām, kas var ietekmēt ieinteresētās personas. Noteikti uzsveriet projekta pozitīvo ietekmi uz organizāciju un tās ieinteresētajām personām.

- Lūdziet ieinteresētajām personām sniegt atsauksmes, lai uzzinātu to intereses un ierosinājumus. Saņemtās atsauksmes iekļaujiet projekta plānošanā un izpildē.
- Ja iespējams, iesaistiet ieinteresētās personas, uzaicinot tās piedalīties sanāksmēs, darbsemināros vai citos pasākumos.
- Cik vien iespējams pārredzami izklāstiet projekta mērķus, problēmas un riskus. Tas veicinās ieinteresēto personu uzticēšanos un radīs lielāku pārliecību par risinājuma sniegto aizsardzību.

Tādēļ ir ļoti svarīgi skaidri noteikt un pienācīgi pārvaldīt ieinteresēto personu funkcijas, pienākumus un iesaisti. Turpmāk 26. attēlā ir sniegts *RASCI* tabulas piemērs, ko var izmantot ieinteresēto personu kartēšanai. Šādu tabulu var paplašināt, ja nepieciešams, un tā jāpielāgo atbilstīgi risinājuma vajadzībām.

25. attēls. RASCI tabulas piemērs, ko nepieciešamības gadījumā var paplašināt

Mērķis	Ieinteresētā persona												
	Uzņēmuma īpašnieks	Vietējie drošības dienesti	Risinājuma operators	Mazināšanas dalībnieki	Tiesībaizsardzība	*C-UAS* risinājuma piegādātājs(-i)	*U-space* pakalpojuma sniedzēji	*UTM* pakalpojuma sniedzēji	Iestādes	Vietējā kopiena	Kaimiņi	Sakaru uzņēmumi	Valsts pārvaldes struktūras
Incidentu pārvaldība													
Dokumentācija un reģistrācija	A	R	R	I	I	I	I	I	I	–	–	–	I
Ieinteresēto personu informēšana													
Iestāžu informēšana													
Tiesu ekspertīzes vākšana													
Riska reģistra atjaunināšana													
Mazināšana													
Saziņa ar pilotiem pasīvai mazināšanai	R	R		R	A	A	R			I		R	R
Informācijas sniegšana par 4G–5G lidojumiem	R	R		R	A	R	R			S		S	S
***UAS* lidojumi**													
Lidojumu apstiprināšana	A	R		I	–	–	I	I	–	–	–	–	–
Lidojumu plānu iekļaušana													
Lidojumu žurnālu atjaunināšana	A	A		A	S	C	A			I		A	A
***UAS* atjaunināšana un darbība**													
Risinājuma darbība													
Vadības un kontroles pārvaldība	A	A		A	R	C	A			I		S	R

Pakalpojumu līmeņa izpildes pārbaudes														
Operatora grafiks														
Incidentu reģistrēšana	A	A		A	S	C	A			I		I	I	
Incidentu, par kuriem ziņots no cita avota, pievienošana žurnālā	C	C		C	A	C	A			C		C	A	
Lidojuma datu novērošana un sniegšana	S	S		S	S	S	S			S		I	S	
Operatoru mācības														
Ieinteresēto personu informēšana														
Uzņēmuma īpašnieka informēšana														
Ielaušanās testi														
Testu plānošana														
Testu izpilde														
Testa dokumentēšana														
Rezultātu paziņošana un ziņošana par tiem														
Risinājuma veiktspēja														
Testu plānošana														
Rezultātu verificēšana														
Testa plāna atjaunināšana														
Kalibrēšana														
Apkope un remonti														
Tehniskās apkopes grafiki														
Pakalpojumu līgumi														

R = atbildīgs	A = pārskatatbildīgs	S = atbalstošs	C = iesaistīts apspriešanā	I = informēts	- = nepiemēro

5.2. *C-UAS* RISINĀJUMA PASTĀVĪGA ATJAUNINĀŠANA

Sagaidāms, ka ikviens *C-UAS* risinājums savā darbības laikā piedzīvos vairākas pārmaiņas: to var skart tādas problēmas kā tehnoloģiju attīstība, tiesiskā regulējuma grozījumi, iekšējās politikas vai procesu izmaiņas vai objekta riska līmeņa pieņemšanas izmaiņas. Visos gadījumos ieteicams rūpīgi uzraudzīt faktorus, kas varētu ietekmēt konkrētu KI objektu vai sabiedrisko vietu. Izveidojot risinājuma ceļvedi, ko uzrauga un pastāvīgi atjaunina, var nodrošināt, ka KI objekta vai sabiedriskās vietas *C-UAS* risinājums atbilst vajadzībām un pienācīgi aizsargā objektu.

PADOMS

Risinājums ir izstrādāts, lai aizsargātu pret konkrētu apdraudējumu un to mazinātu. Mainoties jebkuram elementam, piemēram, apdraudējuma kopskatam, videi, darbības vajadzībām vai drošības līmenim, jāpārskata visi posmi. Ikviena risinājuma pamats ir pamatpasākumu minimums, un, izmantojot tos kopā ar projektēšanas principiem un atvērto arhitektūru, būs vieglāk veikt atjauninājumus un izmaiņas.

KPI var būt efektīva metode, ko izmantot, lai izmērītu risinājuma veiktspēju laika gaitā un redzētu, vai mērķi ir sasniegti. To definēšana vai atlasīšana var būt sarežģīta, un ar *KPI* nedrīkst noteikt tikai tehniskos parametrus, bet ar to jāizmēra aizsardzības līmenis, ko risinājumam bija paredzēts sasniegt. Pienācīgi definēti *KPI* atspoguļos veiktspēju piegādātāju un integratoru izmantotajām sistēmām, un tos var izmantot, lai salīdzinātu risinājumu ar citiem salīdzināmiem ieviestajiem risinājumiem.

Tehnoloģiju attīstība var būt izaicinājums, jo attīstās ne tikai identificēšanas iekārtas un programmatūra, bet arī *UAS*, pret ko jāaizsargā. Piemēram, propelleru konstrukcijas un lidaparāta izgatavošanai izmantotā materiāla izmaiņu dēļ *UAS* var kļūt aizvien grūtāk atklājamas. Regulāri veicot sistēmas testus un ielaušanās testus, būs vieglāk nodrošināt risinājuma piemērotību un atbilstību esošajām vajadzībām.

Izvairīšanās no pakalpojuma sniedzēju piesaistes ir vēl viena vispārpieņemta prakse. Nodrošinot pēc iespējas lielāku sistēmu pamatinfrastruktūras neatkarību no pakalpojuma sniedzējiem, dažādi piegādātāji varēs sniegt pakalpojumus, veikt apkopi un atjauninājumus, kad tas būs nepieciešams.

Strādājot gan ar aparatūras, gan programmatūras integratoriem, risinājumam ir vērts apsvērt modeli "kā pakalpojums", nevis iegūt to īpašumā. Izmantojot modeli "kā pakalpojums", KI objekts vai sabiedriskās vietas galvenā priekšrocība ir iespēja mazināt tehnoloģiju nolietojuma risku. Protams, lai izmantotu šādus ieviešanas modeļus, ir jāveic konkrētā objekta analīze, ņemot vērā citus faktorus, piemēram, tiesiskos regulējumus, datu atrašanās vietu, datu īpašumtiesības, darbības izmaksas, sistēmas uzraudzību un PLV, iekšējo kapacitāti, zinātību un mācību prasības.

PLV noteikti ir rūpīgi jāapsver, un pakalpojuma sniedzējiem un integratoriem tā ir savstarpēji jāsaskaņo. Tie it jāformalizē, sīki izstrādājot pakalpojumu nolīgumu, kurā aprakstīti savstarpējie pienākumi, kā arī *C-UAS* risinājumu apdraudējuma mazināšanas stratēģijas. Arī šajā gadījumā noteikta sistēmas specifikācija un projekts, kas izriet no visaptverošas prasību analīzes, palīdzēs izvairīties no kļūmēm un turpmākām diskusijām, piemēram, par kļūdaini pozitīviem vai kļūdaini negatīviem rezultātiem.

Ierosinātā piektā posma metodika ar to nebeidzas. Kā jau norādīts rokasgrāmatas sākumā, tas ir cirkulārs process, kurā ieviešanas un darbības posmā gūtā pieredze, kā arī apdraudējuma kopuma un iesaistīto tehnoloģiju straujās attīstības dēļ izmantotais risinājums būs pastāvīgi jāpārskata.

12. IZCĒLUMS. DARBĪBAS POSMA KOPSAVILKUMS

Šis ir nepārtraukts risinājuma izmantošanas process. Šajā posmā jums:

- jāuzrauga, lai risinājums atbilstu specifikācijām un aizsargātu pret identificēto risku;
- pastāvīgi jāinformē ieinteresētās personas;
- pastāvīgi jāatjaunina procesi un procedūras;
- jānodrošina risinājuma darbība atbilstīgi darbības vajadzībām, noteikumiem un tiesiskajam regulējumam;
- jāuzrauga darbības vajadzību, tehnoloģiju, ieinteresēto personu, vides, apdraudējuma kopuma utt. izmaiņas un, ja nepieciešamas izmaiņas, no jauna jāizpilda visi šajā rokasgrāmatā minētie posmi, turklāt visa informācija un izmaiņas ir jāreģistrē un pastāvīgi jāatjaunina.

Secinājumi

Pēdējos gados *UAS* jeb tā dēvēto dronu skaits ir strauji pieaudzis. Eiropā un pārējā pasaulē novēro aizvien biežāku *UAS* izmantošanu dažādiem mērķiem. *UAS* izmanto gan civilām darbībām izklaidei, gan komerciālam mērķim jaunos uzņēmējdarbības modeļos, gan arī aizsardzībai.

Šajā rokasgrāmatā ierosināta **piecu posmu metodika**, kas paredzēta KI īpašniekiem un personām, kas atbild par sabiedrisku vietu aizsardzību, kā arī risinājuma izstrāde *UAS* radītā apdraudējuma mazināšanai. Šī metodika sniedz plašu skatījumu uz problēmām, ko *UAS* rada KI un sabiedriskajām vietām. Tā parāda, cik svarīgi ir izstrādāt risinājumus, kas ietver visu vērtību ķēdi – tehnoloģiskās *C-UAS* sistēmās iekļaujot ieinteresēto personu procesus. Tā kā *C-UAS* sistēmās galvenā uzmanība ir pievērta *UAS* atklāšanas, izsekošanas un identificēšanas tehniskajai sarežģītībai, *C-UAS* risinājums ietver visus aspektus un attiecīgās ieinteresētās personas, lai mazinātu *UAS* izraisīto apdraudējumu. Metodikā ir aprakstītas darbības, kas jāņem vērā, izstrādājot *C-UAS* risinājumu.

Pirmajā metodikas **posmā** ir iekļauti ieteikumi par to, kā sākt, saņemot skaidru darbības pilnvarojumu un precīzi definējot mērķus par to, kas, kur un pret ko ir jāaizsargā. Tajā aprakstīti skaidri projektēšanas principi un procesu un procedūru izstrādē iesaistāmās ieinteresētās personas. Šajā posmā ir aprakstīts būtisku pamatpasākumu minimums, kam jābūt visu *C-UAS* risinājumu pamatā.

Otrais posms attiecas uz *UAS* radītajiem riskiem, kas jāiekļauj esošajā risku reģistrā, un tajā izklāstīts, kā aizsargājamajai KI vai sabiedriskajai vietai formulēt attiecīgos konkrētos *UAS* apdraudējuma scenārijus.

Pamatojoties uz šo analīzi, **trešajā posmā** aprakstīts, kā izstrādāt risinājumu, kas atbilst darbības vajadzībām un apzinātajiem riskiem. Tajā aprakstīti svarīgi apsvērumi, kas jāņem vērā, īstenojot pamatpasākumu minimumu, un kā tos izmantot, atlasot pareizo mazināšanas līmeni un pielāgojot nepieciešamās tehnoloģijas. Projektēšanas posma beigās notiek arhitektūras projektēšana, ko varēs izmantot pārrunās ar piegādātājiem (kas ieviesīs risinājumu) un ieinteresētajām personām (kas mazinās riskus).

Pēc tam ir aprakstīts **ceturtais** ieviešanas **posms**. Tajā uzsvērts, ka pirms ieinteresēto personu mācībām un pirms risinājuma pārejas darbības režīmā ir jāveic sistēmas testēšana un ielaušanās testi. Lai nodrošinātu risinājuma efektivitāti un mazināšanu varētu veikt noteiktajā termiņā, ir svarīgi noteikt pareizās ieinteresētās personas. Tā kā salīdzinājumā ar parastajiem drošības pasākumiem *C-UAS,* iespējams, būs jāpiesaista papildu ieinteresētās personas, ir svarīgi ar tām sazināties un iesaistīt jau agrīnā posmā un kopīgi izstrādāt risinājumu, procedūras un procesus.

Piektais posms attiecas uz risinājuma darbību, ieinteresēto personu pastāvīgu informēšanu un risinājuma pastāvīgu atjaunināšanu. Pastāvīga uzraudzība, pienācīgi definēti *KPI* un atjauninājumi nodrošinās, ka tiek pievienotas gan esošās, gan arī jaunas vajadzības, kā arī papildu ieinteresētās personas.

Nepieciešams pilnībā izprast darbības vajadzības saistībā ar *C-UAS*. Plašais un sarežģītais *C-UAS* pasākumu tehnoloģiju formāts var novirzīt uzmanību no sākotnējās darbības problēmas,

kuras dēļ bija jāievieš *C-UAS*. Tā rezultāts var būt neefektīva resursu izmantošana un slikta tehnoloģiju izvēle, kas nespēs nodrošināt nepieciešamo risinājumu.

Pamatpasākumu minimums jāievieš visos risinājumos. Tie veido pamatu, kas nodrošina risinājuma attīstību atbilstīgi mainīgajiem riskiem un darbības vajadzībām. Turklāt konkrētās tehnoloģijas, kas nepieciešamas risku mazināšanai, var būt saistītas, un nepieciešamības gadījumā risinājumu var pārveidot, lai ņemtu vērā vides un riska izmaiņas.

Nav viena risinājuma, kas atbilstu visiem ieviešanas veidiem. Izmantojot noteiktus projektēšanas principus, *C-UAS* risinājumu būs vieglāk iekļaut objekta drošības pasākumos, tādējādi palielinot tā efektivitāti. Katrs metodikas posms ir jāpielāgo konkrētajai videi un riskiem. Visi objekti darbojas atšķirīgā vidē, ar dažādām ieinteresētajām personām, dažādos tirgos, dažādās kopienās utt.

Vides izpētei *UAS* skatījumā ir jāvelta pietiekami daudz laika. Situācijas izpratne, sazinoties ar blakus esošiem KI objektiem, vietējām iestādēm un iedzīvotājiem, atvieglos *C-UAS* risinājuma ieviešanu.

Visbeidzot, *C-UAS* risinājuma izveides process nebeidzas ar šīs metodikas pēdējo posmu. Attīstoties videi, attīstās arī apdraudējuma un tehnoloģiju formāts. Tādēļ piecu posmu metodika ir jāatkārto vairākkārt, lai attiecīgi pilnveidotu *C-UAS* risinājumu.

Saīsinājumu un definīciju saraksts

Saīsinājums vai termins	Apraksts
"Nevērīgo" *UAS* ekspluatantu klasifikācija	*UAS* ekspluatanti, kuri varētu zināt noteikumus, dronu kontroles pasākumus, bet kuri tos, iespējams, neievēro un kuru nodomi ir vieglprātīgi.
"Nezinošo" *UAS* ekspluatantu klasifikācija	*UAS* ekspluatanti, kuri nezina un neievēro noteikumus, *UAS* kontroles pasākumus, *UAS* ekspluatācijas drošību, bet kuru nodomi nav ļaunprātīgi.
"Noziedzīgo" *UAS* ekspluatantu klasifikācija	*UAS* ekspluatanti, kuri varētu zināt noteikumus, dronu kontroles pasākumus, bet tos neievēro un kuru nodomi ir naidīgi.
"Rūpīgo" *UAS* ekspluatantu klasifikācija	*UAS* ekspluatanti, kas zina un ievēro noteikumus, dronu kontroles pasākumus un dronu ekspluatācijas drošību.
Aktīvie pasākumi	Pasākumi, kas izstrādāti, lai fiziski apturētu identificēto *UAS*.
Apdraudējuma analīze	*UAS* apdraudējuma procesa elements, kura mērķis ir izprast *UAS* ekosistēmu.
Apdraudējuma darbības veidu analīze	Apdraudējuma iekļaušanas elements, kas ietver kopējo izpratni par apdraudējumu, analizējot objekta apsekojumu un iespējamo neaizsargātību, lai noteiktu visiespējamāko apdraudējumu un visiedarbīgāko apdraudējuma scenāriju.
Apdraudējuma iedalījums	Šis ir nākamais posms tūlīt pēc *UAS* apdraudējuma procesa. Tajā apraksta taktiskā līmeņa lēmumu pieņemšanas procesu, kas veidos sistēmas reakciju uz neatļautu *UAS* iekļūšanu. Šis posms ir būtiska saikne starp riska novērtējumu un *C-UAS* pasākumu ieviešanu.
Apdraudējuma iekļaušana	*UAS* apdraudējuma procesa elements, kurā izmanto apdraudējuma analīzes secinājumus, lai noteiktu visiespējamāko un bīstamāko *UAS* apdraudējumu.
C-UAS	*UAS* apkarošana ir likumīga un droša bezpilota lidaparātu sistēmu radītu risku atklāšana, izsekošana, identificēšana un mazināšana.
***C-UAS* risinājums**	*C-UAS* risinājums ir *C-UAS* sistēmu un to ekspluatācijā iesaistīto ieinteresēto personu un procesu kopums.
***C-UAS* sistēma**	*C-UAS* sistēma ir *C-UAS* veikšanai izstrādātā risinājuma komponents.
DEW	Virzītās enerģijas ieroči
EO/IR	Elektrooptisks/infrasarkans

Eskalācijas pakāpe	Pastāvošā un pieaugošā risku līmeņa apraksti. Objekts lemj par eskalācijas pakāpju attiecināšanu atbilstīgi riska skaitliskajam novērtējumam, ņemot vērā riska un apdraudējuma analīzē noteikto bīstamību.
GNSS	Globālās navigācijas satelītu sistēmas
IKT	Informācijas un komunikācijas tehnoloģijas
ISO	Starptautiskā Standartizācijas organizācija
JRC	Kopīgais pētniecības centrs
KI	Kritiskā infrastruktūra Aktīvs vai sistēma, kas ir būtiska svarīgu sabiedrības funkciju uzturēšanai.
Kinētiski pasākumi	Kinētiskie mazināšanas paņēmieni bieži ietver noteiktu tiešu fizisku rīcību, lai likvidētu vai mazinātu risku, ko rada *UAS*.
KPI	Galvenais darbības rādītājs
LEA	Tiesībaizsardzības iestāde
PLV	Pakalpojumu līmeņa vienošanās
RASCI	Atbildīgs, pārskatatbildīgs, atbalstošs, iesaistīts apspriešanā, informēts *RASCI* ir matrica (t. i., tabula, modelis vai sistēma), ko izmanto, lai palīdzētu noteikt katras ieinteresētās personas funkcijas un pienākumus projektā. Tajā ir skaidri noteikts, kas izpilda konkrēto projekta apakšuzdevumu.
RF	Radiofrekvence
***RF* traucējumu radīšana**	*RF* traucējumu radīšana pārtrauc *RF* savienojumu starp dronu un tā ekspluatantu, radot plašus *RF* traucējumus. Tiklīdz *RF* savienojums (kas var ietvert *Wi-Fi* savienojumus) pārtrūks, drons parasti vai nu nosēdīsies uz zemes vai sāks manevru "atgriešanās mājās". Tomēr šis paņēmiens nav efektīvs pret droniem, kas darbojas bez aktīva *RF* savienojuma. Daudziem signāla traucētājiem ir arī ierobežots dažus simtus metru plašs darbības diapazons, tāpēc, lai mazinātu traucējošā *UAS* radīto apdraudējumu, sistēmai jāatrodas ļoti tuvu pie tā, un tā nav efektīva, ja nav tiešas redzamības līnijas uz *UAS*. Traucētājiem, kas spēj darboties no liela attāluma un aiz redzamības līnijas, jābūt jaudīgākiem, taču jaudīgāki traucētāji rada arī lielāku risku radīt likumīgu sakaru traucējumus.
Riska skaitliskais novērtējums	Aprēķina, reizinot ietekmes iespējamību.

Riska vadība	*UAS* apdraudējuma procesa elements, kurā piemēro apdraudējuma integrēšanas un apdraudējuma analīzes secinājumus, lai padziļināti izvērtētu KI objekta konkrētos riskus un attiecīgos mazināšanas pasākumus.
Tiešā attālā ID	"Tiešā attālā identifikācija" ir sistēma, kas nodrošina vietēju informācijas pārraidi par ekspluatēto bezpilota lidaparātu, tostarp bezpilota lidaparāta marķējumu, lai šo informāciju varētu iegūt bez tiešas fiziskas piekļuves bezpilota lidaparātam.
Tīkla attālinātā ID	Tīkla attālinātā ID izmanto sakarus ar interneta starpniecību no tīkla attālinātās ID pakalpojumu sniedzēja, kas tieši vai netieši mijiedarbojas ar *UAS* vai ar citiem avotiem neaprīkotu tīkla dalībnieku gadījumā.
UAS	Bezpilota lidaparātu sistēmas Bezpilota lidaparāts un aprīkojums tā attālai vadībai.
***UAS* apdraudējuma process**	Sniedz norādījumus KI pārvaldniekiem, lai palīdzētu izprast un efektīvi pārvaldīt *UAS* riskus.
***UAS* ekspluatants**	Jebkura fiziska persona vai organizācija, kam pieder vai kas nomā *UAS*.
***UAS* ģeogrāfiskā zona**	Gaisa telpas daļa, ko izveidojusi kompetentā iestāde *UAS* operāciju atvieglošanai, ierobežošanai vai aizliegšanai, lai novērstu riskus, kas saistīti ar drošumu, privātumu, personas datu aizsardzību, drošību vai vidi un kas izriet no *UAS* operācijām.
***UAS* risku reģistrs**	Identificēto risku saraksts, iedalīts atbilstīgi katra apdraudējuma veida izvirzītajai problēmai.
UTM	Bezpilota lidaparātu sistēmu satiksmes vadība Starptautiskā Civilās aviācijas iestāde *UTM* plašākā nozīmē definē kā "īpašu gaisa satiksmes pārvaldības aspektu, kas *UAS* operācijas pārvalda droši, ekonomiski un efektīvi, nodrošinot iekārtas un vienotu pakalpojumu kopumu sadarbībā ar visām pusēm un iesaistot funkcijas, ko veic gaisā un uz zemes". Tāpēc *UTM* sistēma "nodrošina *UTM*, sadarbīgi integrējot cilvēkus, informāciju, tehnoloģiju, telpas un pakalpojumus, ko atbalsta gaisa, zemes vai kosmosa sakari, navigācija un uzraudzība".
Uzlaušana	Uzlaušana notiek, pārņemot *UAS* operētājsistēmas pamatprivilēģijas un veicot attiecīgas darbības. Šīs metodes trūkums ir tas, ka to var izmantot tikai konkrētām operētājsistēmām un tīkla protokoliem un, tāpat kā *RF* traucēšana, tā ietekmē citas rūpnieciskās, zinātniskās un medicīniskās ierīces, kas izmanto attiecīgo joslu.

Viltošana	Nodrošina iespēju pārņemt mērķa *UAS* vadību vai to pārvirzīt ar viltus saziņu vai navigācijas saiti. Tomēr viltošanas sistēmas ir ļoti tehniski sarežģīti izveidot un ieviest, un tās var nebūt vienlīdz efektīvas pret visām *UAS*. Piemēram, bezpilota lidaparāti, kas izgatavoti ar aizsargātām sakaru saitēm, var būt noturīgi pret viltošanas mēģinājumiem.
VIP	Ļoti svarīga persona Ļoti svarīga vai ietekmīga persona, pret kuru jāizturas īpaši.

Izcēlumu saraksts

Attēlu saraksts

SAZIŅA AR ES

KLĀTIENĒ

Eiropas Savienībā ir simtiem *Europe Direct* centru. Tuvākā centra adresi varat skatīt tiešsaistē (european-union.europa.eu/contact-eu/meet-us_en).

PA TĀLRUNI VAI RAKSTVEIDĀ

Europe Direct ir dienests, kas darbojas, lai palīdzētu jums rast atbildes uz jautājumiem par Eiropas Savienību. Jūs varat sazināties ar šo dienestu:

- **pa bezmaksas tālruni**: 00 800 6 7 8 9 10 11 (atsevišķi operatori var piemērot maksu par šiem zvaniem);
- **zvanot uz standarta numuru:** +32 22999696;
- **izmantojot šeit pieejamo veidlapu**: european-union.europa.eu/contact-eu/write-us_en.

UZZINĀT INFORMĀCIJU PAR ES

TIEŠSAISTĒ

Informācija par Eiropas Savienību visās oficiālajās ES valodās ir pieejama Eiropas tīmekļvietnē (european-union.europa.eu).

ES PUBLIKĀCIJAS

ES publikācijas varat skatīt vai pasūtīt op.europa.eu/en/publications. Vairākus bezmaksas publikāciju eksemplārus varat iegūt, sazinoties ar *Europe Direct* vai vietējo informācijas centru (european-union.europa.eu/contact-eu/meet-us_en).

ES TIESĪBU AKTI UN SAISTĪTIE DOKUMENTI

Lai piekļūtu ES juridiskajai informācijai, tostarp visiem ES tiesību aktiem, kas publicēti kopš 1951. gada visu valsts valodu redakcijās, apmeklējiet vietni *EUR-Lex*(eur-lex.europa.eu).

ATVĒRTIE DATI NO ES

Portālā data.europa.eu var piekļūt atvērtām datu kopām no ES iestādēm, struktūrām un aģentūrām. Šos datus var lejupielādēt un atkārtoti izmantot bez maksas gan komerciālām, gan nekomerciālām vajadzībām. Portāls arī nodrošina piekļuvi plašam Eiropas valstu datu kopu klāstam.

Eiropas Komisijas zinātnes un zināšanu dienesta
Kopīgais pētniecības centrs

***JRC* uzdevums**
Kopīgā pētniecības centra – Eiropas Komisijas zinātnes un zināšanu dienesta – uzdevums ir atbalstīt ES politiku, visā politikas veidošanas ciklā sniedzot neatkarīgus pierādījumus.

EU Science Hub
joint-research centre.ec.europa.eu

@EU_ScienceHub

EU Science Hub-Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

EU Science

Publications Office
of the European Union